取扱説明書 - 日本語

FUJITSU Software ServerView Suite

Remote Management

iRMC S4 - integrated Remote Management Controller

2013 年 8 月版

製品名称の表記

本書では、本文中の製品名称を、次のように略して表記します。

製品名称	本文中の表記	
Microsoft® Windows Server® 2008 Standard Microsoft® Windows Server® 2008 Enterprise Microsoft® Windows Server® 2008 Datacenter Microsoft® Windows Server® 2008 Foundation Microsoft® Windows® Small Business Server 2008 Standard Microsoft® Windows® Small Business Server 2008 Premium	Windows Server 2008	Windows
Microsoft® Windows Server® 2008 R2 Standard Microsoft® Windows Server® 2008 R2 Enterprise Microsoft® Windows Server® 2008 R2 Datacenter Microsoft® Windows Server® 2008 R2 Foundation Microsoft® Windows® Web Server 2008 R2	Windows Server 2008 R2	
Microsoft® Windows Server® 2003, Standard Edition Microsoft® Windows Server® 2003, Enterprise Edition Microsoft® Windows Server® 2003, Enterprise Edition for Itanium-based Systems Microsoft® Windows® Small Business Server 2003	Windows Server 2003	
Microsoft® Windows Server® 2003, Standard x64 Edition Microsoft® Windows Server® 2003, Enterprise x64 Edition	Windows Server 2003 x64	
Microsoft® Windows Server® 2003 R2 Standard Edition Microsoft® Windows Server® 2003 R2 Enterprise Edition Microsoft® Windows® Small Business Server 2003 R2 Microsoft® Windows® Storage Server 2003 R2, Standard Edition	Windows Server 2003 R2	
Microsoft® Windows Server® 2003 R2 Standard x64 Edition Microsoft® Windows Server® 2003 R2 Enterprise x64 Edition	Windows Server 2003 R2 x64 または Windows Server 2003 R2	
Microsoft® Windows Server® 2012 Foundation Microsoft® Windows Server® 2012 Standard Microsoft® Windows Server® 2012 Datacenter	Windows Server 2012	

<table>
<tr><th>製品名称</th><th colspan="3">本文中の表記</th></tr>
<tr><td>Red Hat Enterprise Linux 5</td><td>RHEL5</td><td rowspan="3">Red Hat Linux</td><td rowspan="5">Linux</td></tr>
<tr><td>Red Hat Enterprise Linux AS（v.4）</td><td rowspan="2">RHEL4</td></tr>
<tr><td>Red Hat Enterprise Linux ES（v.4）</td></tr>
<tr><td>SUSE Linux Enterprise Server 11</td><td>SuSE Linux SLES11
または SLES11</td><td rowspan="2">SuSE Linux</td></tr>
<tr><td>SUSE Linux Enterprise Server 10</td><td>SuSE Linux SLES10
または SLES10</td></tr>
<tr><td>VMware ESX 4</td><td colspan="2">ESX4</td><td rowspan="2">VMware</td></tr>
<tr><td>VMware ESX 3.5</td><td colspan="2">ESX3.5</td></tr>
</table>

著作権および商標

Copyright © 2013 Fujitsu Technology Solutions GmbH.

All rights reserved

Microsoft、Windows、Windows Server、Hyper-V は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標あるいは商標です。

Red Hat および Red Hat をベースとしたすべての商標とロゴは、米国およびその他の国における Red Hat, Inc. の商標または登録商標です。

BrightStor, ARCserve は、CA, Inc の登録商標です。

VMware、VMware ロゴ、VMware ESXi、VMware SMP および VMotion は VMware,Inc の米国およびその他の国における登録商標または商標です。

その他の各製品名は、各社の商標、または登録商標です。

その他の各製品は、各社の著作物です。

目次

1 はじめに 11

1.1 このマニュアルの目的と対象ユーザ 12
1.2 iRMC S4 の機能（概要） 13
1.3 iRMC S4 の通信インタフェース 20
1.4 iRMC S4 で使用される通信プロトコル 21
1.5 IPMI - 技術的背景 22
1.6 DCMI（データセンター管理インターフェース） 30
1.7 ServerView Suite リンク集 31
1.8 ServerView Suite のマニュアル 32
1.9 表記規約 33

2 iRMC S4 への初回ログオン 35

2.1 要件 35
2.2 iRMC S4 の工場出荷時のデフォルト 36
2.3 iRMC S4 Web インターフェースへのログイン 37

3 iRMC S4 の設定 39

3.1 iRMC S4 の LAN インターフェースの設定 39
3.1.1 前提条件 40
3.1.1.1 正しい LAN ポートへの接続 40
3.1.1.2 iRMC S4 とシステムの IP アドレス間の相互動作 . . . 41
3.1.1.3 他のサブネットからのアクセス 41
3.1.2 LAN インターフェースの設定：Configuration Tools 41
3.1.3 UEFI セットアップユーティリティを使用した LAN インターフェースの設定 42
3.1.4 LAN インターフェースのテスト 43

3.2 UEFI セットアップユーティリティを使用した LAN 経由のテキストコンソールリダイレクションの設定 44
3.2.1 iRMC S4 のテキストコンソールリダイレクションの設定 . 45

3.2.2 オペレーティングシステム実行中のコンソールリダイレクションの使用 47

3.3 iRMC S4 のシリアルインターフェースの設定と使用 . . . 49
3.3.1 iRMC S4 を使用したシリアルインターフェースの設定 . . 49
3.3.2 リモートマネージャ（シリアル）の使用 51

3.4 iRMC S4 Web インターフェースによる iRMC S4 の設定 . 52
3.4.1 LAN パラメータの構成 52
3.4.2 通知の設定 53
3.4.3 テキストコンソールリダイレクションの構成 53

4 iRMC S4 のユーザ管理 55

4.1 iRMC S4 によるユーザ管理の概念 56

4.2 ユーザ権限 58

4.3 iRMC S4 のローカルユーザ管理 60
4.3.1 iRMC S4 Web インターフェースを使用したローカルユーザ管理 60
4.3.2 Server Configuration Manager でのローカルユーザ管理 . . 61
4.3.3 iRMC S4 ユーザの SSHv2 公開鍵認証 62
4.3.3.1 SSHv2 の公開鍵と秘密鍵の作成 63
4.3.3.2 SSHv2 鍵のファイルから iRMC S4 へのアップロード . 67
4.3.3.3 PuTTY と OpenSSH クライアントが公開 SSHv2 鍵を使用するための設定 69
4.3.3.4 例 : 公開 SSHv2 鍵 74

5 ビデオリダイレクション（AVR） 75

5.1 要件 : AVR 設定の確認 76

5.2 AVR の使用 78
5.2.1 AVR ウィンドウ 79
5.2.2 低帯域幅の使用 80
5.2.3 同時 AVR セッション 80
5.2.4 「サーバ側モニタの表示オフ制御」機能 82
5.2.5 キーボードリダイレクション 83
5.2.6 マウスリダイレクション 85

5.3 AVR ウィンドウのメニューとツールバー 86
5.3.1 「ビデオ」メニュー 87
5.3.2 AVR ウィンドウ - 「キーボード」メニュー 91
5.3.3 AVR ウィンドウ - 「マウス」メニュー 96
5.3.4 AVR ウィンドウ - 「オプション」メニュー 98
5.3.5 AVR ウィンドウ - 「メディア」メニュー 100
5.3.6 AVR ウィンドウ - 「電力制御」メニュー 101
5.3.7 AVR ウィンドウ - 「アクティブユーザ」メニュー 103
5.3.8 AVR ウィンドウ - 「ヘルプ」メニュー 103
5.3.9 AVR ツールバー 105

6 仮想メディアウィザード 109

6.1 リモートワークステーションへのバーチャルメディアの提供 110
6.1.1 Virtual Media ウィザードの起動 111
6.1.2 「Virtual Media」ダイアログボックス 112
6.1.3 バーチャルメディアへのストレージメディアの提供 . . . 114
6.1.4 バーチャルメディア接続のクリア 117

7 iRMC S4 Web インターフェース 119

7.1 iRMC S4 Web インターフェースへのログイン 120

7.2 必要なユーザ権限 123

7.3 ユーザインターフェースの構造 128

7.4 システム情報 -
管理対象サーバの情報 131
7.4.1 システムの概要 -
サーバの一般情報 132
7.4.2 システム構成情報 -
サーバ構成情報 137
7.4.3 Network Inventory 140

7.5 「RAID 情報」-
RAID システムに関する情報 141
7.5.1 「RAID コントローラ」- RAID コントローラおよび関連す
るバッテリーに関する情報 142
7.5.2 「物理ディスク」- RAID 物理ディスクに関する情報 . . . 144
7.5.3 「論理デバイス」-
RAID 論理ドライブに関する情報 146

7.6 BIOS - BIOS 設定のバックアップ / リストア、BIOS のフラッシュ . . . 148
7.6.1 バックアップ / リストア - BIOS パラメータ設定のファイルへの保存 / ファイルへのリストア . . . 148
7.6.1.1 単一の BIOS パラメータの ServerView® WinSCU XML 形式でのバックアップ . . . 149
7.6.1.2 単一の BIOS パラメータの ServerView® WinSCU XML 形式での復元 . . . 151
7.6.2 BIOS アップデート - 「ファイルからアップロード」するか TFTP 経由での BIOS のアップデート . . . 153

7.7 iRMC S4 - 情報、ファームウェアおよび認証 . . . 158
7.7.1 「iRMC S4 情報」- iRMC S4 上の情報 . . . 159
7.7.2 「iRMC S4 時刻」- iRMC S4 の時刻オプション . . . 163
7.7.3 「iRMC S4 ファームウェア設定の保存」- ファームウェア設定の保存 . . . 166
7.7.4 認証データアップロード - DSA/RSA 証明書および DSA/RSA 秘密鍵のアップロード . . . 168
7.7.5 自己署名 RSA 証明書の作成 . . . 175
7.7.6 iRMC S4 ファームウェアアップデート . . . 177

7.8 電源制御 . . . 182
7.8.1 電源投入 / 切断 ―サーバの自動電源投入 / 切断 . . . 183
7.8.2 電源制御オプション - サーバの電源制御の構成 . . . 187
7.8.3 電源装置情報 - 電源装置および FRU コンポーネントの IDPROM データ . . . 190

7.9 電力制御 . . . 191
7.9.1 消費電力制御 - サーバの消費電力制御 . . . 192
7.9.2 現在のシステム消費電力 - 消費電力の表示 . . . 198
7.9.3 消費電力モニタリング履歴 - 消費電力の表示 . . . 199

7.10 センサ - センサの状態確認 . . . 203
7.10.1 ファン - ファン状態確認 . . . 204
7.10.2 温度 - サーバコンポーネントの温度のレポート . . . 206
7.10.3 電圧 - 電圧センサ情報のレポート . . . 208
7.10.4 電源装置個別情報 - 電源ユニットの状態確認 . . . 209
7.10.5 コンポーネント - サーバコンポーネントの状態確認 . . . 211

7.11　イベントログ 214
7.11.1　システムイベントログ内容 - SEL および SEL エントリに関する情報の表示 215
7.11.2　イベントログ情報 - 内部イベントログと関連するエントリに関する情報の表示 . 218
7.11.3　システムイベントログ設定 - IPMI SEL と内部イベントログの設定 221

7.12　サーバ管理情報 - サーバ設定の編集 224

7.13　ネットワーク設定 - LAN パラメータの編集 229
7.13.1　Network Interface - iRMC S4 上の Ethernet 設定の編集 230
7.13.2　ポート番号とネットワークサービス - ポートとネットワークサービスの設定 237
7.13.3　DNS 構成 - iRMC S4 の DNS の設定 240

7.14　通知情報設定 - 警告通知の設定 244
7.14.1　SNMP トラップ送信設定 - SNMP トラップ通知の設定 245
7.14.2　Email 設定 - Email 送信設定 246

7.15　ユーザ管理 252
7.15.1　ユーザ管理 - iRMC S4 のローカルユーザ管理 252
7.15.1.1　新規ユーザの構成 - 新規ユーザの構成 254
7.15.1.2　「ユーザ “<name>” 構成」- ユーザ設定（詳細） 255
7.15.2　ディレクトリサービス構成 - iRMC S4 でディレクトリサービスの設定 262
7.15.2.1　Microsoft Active Directory 用の iRMC S4 の設定 . . . 265
7.15.2.2　iRMC S4 の Novell eDirectory/OpenLDAP/OpenDS/ Open DJ のための設定 269
7.15.3　Centralized Authentication Service（CAS）設定 - CAS サービスの設定 276

7.16　コンソールリダイレクション - コンソールのリダイレクト . 283
7.16.1　BIOS テキストコンソール - テキストコンソールリダイレクションの設定と開始 . . . 283
7.16.1.1　BIOS コンソールリダイレクションオプション - テキストコンソールリダイレクションの設定 284
7.16.1.2　オペレーティングシステム実行中のテキストコンソールのリダイレクション 286
7.16.2　ビデオリダイレクション（AVR） - ビデオリダイレクション（AVR）の開始 288

7.17 ヴァーチャルメディア 296
7.17.1 「ヴァーチャルメディアオプション」- 仮想メディアオプションの設定 297
7.17.2 「リモートイメージマウント」- リモート ISO イメージへの接続 299

8 Telnet/SSH 経由の iRMC S4 (リモートマネージャ) 303

8.1 管理対象サーバに関する要求 304
8.2 リモートマネージャの操作 305
8.3 メニューの概要 306
8.4 ログイン 309
8.5 リモートマネージャのメインメニュー 311
8.6 必要なユーザ権限 313
8.7 Change Password 315
8.8 システム情報 - 管理対象サーバの情報 315
8.9 電源制御 317
8.10 Enclosure Information - システムイベントログとセンサの状態 318
8.11 サービスプロセッサ - IP パラメータ、識別灯、iRMC S4 リセット 323
8.12 RAID Management 324
8.13 Console Redirection (EMS/SAC) - テキストコンソールリダイレクションの開始 325
8.14 コマンドラインシェルの起動 ...- SMASH CLP シェルの起動 325
8.15 Console Logging - メッセージ出力のテキストコンソールへのリダイレクト（シリアル） 326
8.16 コマンドラインプロトコル (CLP) 328

9 Server Configuration Manager を使用した iRMC S4 の設定 333

9.1 ServerView Installation Manager からの Server Configuration Manager の呼び出し 335

9.2 Windows スタートメニューからの Server Configuration Manager の呼び出し 335

9.3 Operations Manager からの Server Configuration Manager の呼び出し 337

10 ファームウェアの更新 341

10.1 iRMC S4 ファームウェア（概要） 342

10.2 USB メモリスティックの設定 344

10.3 ファームウェアイメージのアップデート 347

10.3.1 iRMC S4 Web インターフェースを使用したアップデート . 348

10.3.2 ServerView Update Manager を使用したアップデート . . 348

10.3.3 ServerView Update Manager Express または ASP を使用するオンラインアップデート 349

10.3.4 オペレーティングシステムのフラッシュツールを使用してアップデートする 350

10.3.5 FlashDisk メニューによるアップデート 352

10.4 エマージェンシーフラッシュ 355

10.5 フラッシュツール 356

11 iRMC S4 によるオペレーティングシステムのリモートインストール 361

11.1 iRMC S4 を使用したオペレーティングシステムのインストール - 基本手順 362

11.2 バーチャルメディアとしてのストレージメディアの接続 . . 364

11.3 管理対象サーバを ServerView Suite DVD から起動して、Installation Manager で設定する 367

11.4 設定完了後の管理対象サーバへの OS のインストール . . 370

11.4.1 設定完了後の管理対象サーバへの Windows のインストール . 370

11.4.2 設定完了後の管理対象サーバへの Linux のインストール . . 372

12 付録 375

12.1 iRMC S4 でサポートされる IPMI OEM コマンド 375
12.1.1 概要 375
12.1.2 IPMI OEM コマンドの記述 377
12.1.2.1 記述形式 377
12.1.2.2 SCCI 準拠の自動電源投入／電源切断コマンド 378
12.1.2.3 SCCI 準拠の通信コマンド 384
12.1.2.4 SCCI 準拠のシグナリングコマンド 386
12.1.2.5 Firmware 特有のコマンド 387
12.1.2.6 BIOS 特有のコマンド 391
12.1.2.7 iRMC S4 特有のコマンド 393

12.2 SCCI およびスクリプト設定を使用した iRMC S4 の設定 . . 404
12.2.1 iRMC S4 設定データ 404
12.2.1.1 概要 404
12.2.1.2 SCCI ファイルフォーマット 406
12.2.1.3 注意事項 411
12.2.1.4 iRMC S4 からのエクスポート /iRMC S4 へのインポート . 412
12.2.2 iRMC S4 のスクリプト設定 413
12.2.2.1 iRMC S4 でサポートされる SCCI コマンドの一覧 . . . 413
12.2.2.2 cURL でのスクリプティング 414
12.2.2.3 Visual Basic（VB）スクリプトでのスクリプティング . 415
12.2.2.4 Python でのスクリプティング 416
12.2.2.5 iRMC_PWD.exe プログラムでの暗号化パスワードの生成 417

1　はじめに

最近のサーバシステムはますます複雑化しています。それに従って、このようなシステムの管理に関する要件は拡大しつつあります。

この成長に応じて、いくつかのベンダーが、中央システムコントローラ（Baseboard Management Controller - BMC）とプラットフォーム管理用のインテリジェントハードウェアの間の標準化され、抽象的で、メッセージベースのインターフェースを定義することを目標とした IPMI（「インテリジェントプラットフォーム管理インターフェース」）イニシアチブを設立しました。IPMI に関して詳しくは、22 ページ の「IPMI - 技術的背景」の項 を参照してください。

iRMC（**i**ntegrated **R**emote **M**anagement **C**ontroller）S4 は、統合された LAN 接続と拡張機能を持つ BMC を表します。このように、iRMC S4 は PRIMERGY サーバをシステムのステータスに関係なく包括的に制御する機能を提供します。特に、iRMC S4 では、PRIMERGY サーバの帯域外管理（Lights Out Management - LOM）が可能です。帯域外管理では、サーバの電源がオンになっているかどうかに関係なくシステム管理者がリモート制御を使用してサーバを監視および管理できるようにする専用の管理チャネルを使用します。

図 1: PRIMERGY サーバのシステムボード上の iRMC S4

最近の PRIMERGY サーバのシステムボードにある自律型のシステムとして、iRMC S4 は独自のオペレーティングシステム、独自の Web サーバ、分離されたユーザ管理、および独立したアラート管理を備えています。サーバがスタンバイモードになっていても、iRMC S4 の電源は入った状態で維持されます。

このマニュアルでは、iRMC S4 および使用可能なさまざまなユーザインターフェースを設定する方法について説明します。

1.1 このマニュアルの目的と対象ユーザ

このマニュアルは、ハードウェアとソフトウェアとについて十分な知識を持っているシステム管理者、ネットワーク管理者、およびサービス専門家を対象とします。IPMI の背景にあるテクノロジーに関する基本的な情報と、以下の事項について詳しく扱います。

- iRMC S4 へのログオン
- iRMC S4 の設定
- iRMC S4 上のユーザ管理
- iRMC S4 を使用したビデオリダイレクション
- iRMC S4 を使用したバーチャルメディア
- iRMC S4 Web インターフェース
- iRMC S4 の Telnet/SSH ベースのインターフェース（リモートマネージャ）
- Server Configuration Manager を使用した iRMC S4 の設定
- ファームウェアのアップデート
- iRMC S4 によるオペレーティングシステムのリモートインストール
- 付録の IPMI OEM コマンド
  - IPMI OEM コマンド
  - SCCI およびスクリプト設定を使用した iRMC S4 の設定

サービス

PRIMERGY サーバに対するリモート管理について質問がおありの場合は、担当のサービスおよびサポートパートナーにお問い合わせください。

その他の情報

http://www.ts.fujitsu.com

1.2 iRMC S4 の機能（概要）

iRMC S4 では、提供される広範囲の機能をデフォルトでサポートしています。ビデオリダイレクション（AVR）とバーチャルメディアを使用すると、iRMC S4 では、PRIMERGY サーバのリモート管理に 2 つの追加機能も提供されます。AVR とバーチャルメディアを使用するには、別売りの有効なライセンスキーが必要です。

iRMC S4 **の機能**

- ブラウザによるアクセス

  iRMC S4 は、管理サーバによって標準的な Web ブラウザからアクセスできる独自の Web サーバを備えています。

- セキュリティ（SSL、SSH）

  Web サーバへのセキュアな通信と、マウスやキーボードを含む安全なグラフィカルコンソールリダイレクションを、HTTPS/SSL を使用して提供できます。リモートマネージャを使用して iRMC S4 にアクセスするように、SSH メカニズムを使用して保護され、暗号化された接続を設定できます。リモートマネージャは、iRMC S4 用の英数字によるユーザインターフェースです。

- ServerView 統合

  ServerView エージェントが iRMC S4 を検出し、自動的に関連サーバに適用します。したがって ServerView リモートマネジメントフロントエンドを使って、ServerView Operations Manager から iRMC S4 Web インターフェースおよびテキストコンソールリダイレクトを直接開始できます。

- 電源管理

  システムのステータスに関係なく、リモートワークステーションから管理対象サーバの電源オン / オフを以下の方法で切り替えることができます。

  – iRMC S4 Web インターフェースを使用する
  – Remote Manager　またはコマンドライン・インターフェース (CLP) を使用する
  – スクリプトで行う

- 消費電力管理

  iRMC S4 では、管理対象サーバに対する包括的な消費電力制御を行うことができます。また、iRMC S4 が管理対象サーバに対して電力消費を制御するために使用するモード（最低電力消費または最高パフォーマンス）を指定できます。これらのモードは必要に応じて切り替えることができます。

- 顧客自己保守（CSS）

  iRMC S4 Web インターフェースのサーバコンポーネント、センサ、電源のサマリ表には、影響を受けるサーバコンポーネントが CSS コンポーネントであるかどうかに関して個別の列に情報が表示されます。また、システムイベントログ（SEL）のエラーリストに、CSS コンポーネントによってトリガされたかどうかがすべてのイベントについて示されます。

- テキストコンソールリダイレクション

  ServerView Remote Management Frontend から iRMC S4 への Telnet/SSH セッションを開始できます。これにより、リモートマネージャが呼び出され、テキストコンソールリダイレクションセッションを開始できます。

- BMC　の基本的な機能

  iRMC S4 は、電圧監視、イベントログ、リカバリ制御など、BMC の基本的な機能をサポートしています。

- 「ヘッドレス」のシステム動作

  管理対象サーバにマウス、モニタ、キーボードを接続する必要はありません。これには、コストが削減され、ケーブル配線がシンプルになり、セキュリティが向上するなどのメリットがあります。

- ID LED

  たとえば、フル装備のラックに取り付けられた場合に、システムの識別を容易にするために、iRMC S4 Web インターフェースから ID LED を有効にすることができます。

- 保守ランプ

  保守 LED は、管理対象システムのステータスを知らせると同時に、CSS（Customer Self Service）ステータスを示します。

- Power LED

  Power LED は、サーバのスイッチが現在オンになっているか、オフになっているかを知らせます。

- LAN

  システムによって、サーバに装着されているシステム NIC（Network Interface Card）が管理 LAN 用に予約されているものもあれば、LAN インターフェースを以下のように設定することを選択できるものもあります。

  – 管理 LAN 用に予約する
  – システムと操作を共有するように設定する
  – システムから完全に使用可能にする

  スパナのマークが付いているポートが iRMC S4 に割り当てられています（40 ページ の図 7 を参照）。

- ネットワークボンディング

  iRMC S4 のネットワークボンディングは、Ethernet ネットワーク アダプタの故障時の冗長を目的として設計されています。そのため、iRMC S4 ネットワーク管理のトラフィックは、単一の物理リンクの故障によって発生するサービスロスから保護されます。

  iRMC S4 はアクティブバックアップモードをサポートします。つまり、リンクが故障するまで一方のポートがアクティブで、リンクが故障するともう一方のポートが MAC を引き継いでアクティブになります。

- コマンドラインインタフェース (CLP)

  リモートマネージャに加えて、iRMC S4 では、DMTF（Distributed Management Task Force）によって標準化された SMASH CLP（**S**ystem **M**anagement **A**rchitecture for **S**erver **H**ardware **C**ommand **L**ine **P**rotocol）をサポートしています。

- シンプルな設定 - インタラクティブ / スクリプトベース

  iRMC S4 の設定には、以下のツールが使用できます。

  – iRMC Web インターフェース
  – Server Configuration Manager
  – UEFI BIOS セットアップ

  Server Configuration Manager または IPMIVIEW でスクリプトを使用して設定を実行することもできます。これは、サーバがまず ServerView Installation Manager を介して設定されるときに iRMC S4 を設定することが可能なことを意味します。スクリプトに基づいて多数のサーバを設定することも可能です。

- LocalView Service Panel のサポート

  PRIMERGY サーバに ServerView Local Service Panel, が搭載されている場合、このモジュールにより、どのモジュールが故障しているか、および故障しているモジュールを自分で交換できるかどうかを判断できます。

- ローカルユーザ管理

  iRMC S4 には、固有のユーザ管理方法があり、最大 16 人のユーザをパスワード付きで作成し、それぞれが属するユーザグループによってさまざまな権限を割り当てることができます。

- ディレクトリサービスを使用するグローバルユーザ管理

  iRMC S4 のグローバルユーザ ID は、ディレクトリサービスのディレクトリに保管されています。これにより、集中サーバによるユーザ ID 管理が可能となっています。そのため、ネットワークでこのサーバに接続されているすべての iRMC S4 で、ユーザ ID を使用することができます。

  iRMC S4 ユーザ管理では、現在以下のディレクトリサービスがサポートされます。

  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP[OpenLDAP]
  – OpenDS[OpenDS]

- CAS ベースのシングルサインオン（SSO）認証

  iRMCS4 は CAS（Centralized Authentication Service）設定をサポートしており、CAS ベースのシングルサインオン（SSO）認証用の iRMC S4 Web インターフェースを設定できます。

  CAS サービスの SSO ドメイン内のアプリケーションに初めてログインすると（iRMC S4 Web インターフェースなど）、CAS 固有のログイン画面でログイン認証情報の入力が要求されます。CAS サービスによる認証に成功すると、ユーザはログイン認証情報を再び入力せずに、iRMC S4 Web インターフェースと SSO ドメイン内の他のサービスへのアクセスが許可されます。

- DNS / DHCP

  iRMC S4 は、自動ネットワーク設定をサポートしています。これにはデフォルトの名前があり、DHCP サポートは iRMC S4 が DHCP サーバから IP アドレスを取得するようにデフォルトで設定されています。iRMC S4 名は、DNS（Domain Name Service）によって登録されます。最大 5 つの DNS サーバがサポートされています。DNS/DHCP が使用できない場合、iRMC S4 は静的 IP アドレスもサポートしています。

- 電源の供給

  iRMC S4 は、システムのスタンバイ電源を使用して電源が供給されます。

- アラート管理

  iRMC S4 のアラート管理機能は、アラート転送（警告通知）のために以下のオプションを提供しています。

  – SNMP を使用して PET（Platform Event Trap）が送信されます。
  – 電子メールで直接アラートを送信します。

  また、iRMC S4 は、関連するすべての情報を ServerView エージェントに供給します。

- システムイベントログ（SEL）の読み取り、フィルタ、保存

  次の方法で、SEL の内容を表示、保存、削除できます。

  – iRMC S4 Web インターフェースを利用

  – iRMC S4 の Telnet/SSH ベースのインターフェース（リモートマネージャ）を利用

- iEL（iRMC Event Log : 内部イベントログ）の表示、フィルタリングおよび退避

  次の方法で、iEL の内容を表示および退避し、削除できます。

– iRMC S4 Web インターフェースを利用

– iRMC S4 の Telnet/SSH ベースのインターフェース（リモートマネージャ）を利用

iRMC S4 の拡張された機能

標準的な機能とは別に、iRMC S4 はバーチャルメディア機能とリモートストレージ機能もサポートしています。

- ビデオリダイレクション（AVR）

  iRMC S4 はビデオリダイレクション（AVR）をサポートし、次の利点があります。

  – 標準的な Web ブラウザ上での操作。Java Runtime Environment 以外の追加ソフトウェアを管理サーバにインストールする必要がありません。

  – システムに依存しないグラフィカルおよびテキストコンソールリダイレクション（マウスおよびキーボードを含む）。

  – ブート監視、BIOS 管理、およびオペレーティングシステムの操作のためのリモートアクセス。

  – AVR は、他の場所からサーバを操作するための最大 2 つの同時「仮想接続」をサポートしています。また、ハードウェアおよびビデオ圧縮を使用してネットワーク上の負荷を削減します。

  – ローカルモニタの電源切断のサポート : AVR セッション中にローカルサーバ画面で実行されるユーザ入力およびアクションを権限のない者が見ることができないようにするために、AVR セッション中に管理対象の PRIMERGY サーバのローカル画面の電源を切断することが可能です。

  – 低帯域幅

    データ転送速度が低下した場合、現在の AVR セッションの色深度に対する帯域幅（bpp、ビット / ピクセル）を低く設定できます。

- バーチャルメディア

  バーチャルメディア機能により、リモートのワークステーションに物理的に存在しているか、*Remote Image Mount* 機能を使用したネットワークで一元的に使用可能な「仮想」ドライブが使用できます。

  ヴァーチャルメディアで使用可能な「仮想」ドライブは、ローカルドライブとほぼ同じ方法で管理され、以下の選択肢を提供します。

  – データの読み取りおよび書き込み。
  – ヴァーチャルメディアからのブート。
  – ドライバおよび小規模のアプリケーションのインストール。
  – リモートワークステーションからの BIOS のアップデート。
  （USB を使用した BIOS のアップデート）

  バーチャルメディアは、以下の種類のデバイスをサポートして、リモートワークステーション上の「仮想ドライブ」を提供します。

  – CD ROM
  – DVD ROM
  – メモリスティック
  – Floppy イメージ
  – CD ISO イメージ
  – DVD ISO イメージ
  – 物理ハードディスクドライブ
  – HDD ISO イメージ

  Remote Image Mount 機能により、ISO イメージは「仮想ドライブ」という形態でネットワーク共有に一元的に提供されます。

1.3 iRMC S4 の通信インタフェース

iRMC S4 は以下のような通信インタフェースを提供します :

- **iRMC S4 Web インターフェース (web interface)**

  iRMC S4 Web サーバへの接続は、標準的な Web ブラウザ（Microsoft Internet Explorer、Mozilla Firefox など）を使用して確立します。

  特に、iRMC S4 の Web インターフェースにより、すべてのシステム情報およびファン速度、電圧などのセンサからのデータにアクセスできます。テキストベースのコンソールリダイレクションおよびグラフィカルコンソールリダイレクション（ビデオリダイレクション - AVR）を設定することもできます。また、管理者は Web インターフェースを使用して iRMC S4 全体を設定できます。HTTPS/SSL で iRMC S4 Web サーバへのセキュアなアクセスを実現できます。

  Web インタフェースを使用した iRMC S4 の操作については、119 ページ の「iRMC S4 Web インターフェース」の章を参照してください。

- **リモートマネージャ : LAN を使用したテキストベースの Telnet/SSH インターフェース**

  リモートマネージャを次の方法で呼び出すことができます。

  – ServerView Remote Management Frontend から。
  – Telnet/SSH クライアントから直接。

  リモートマネージャの英数字ユーザインターフェースからは、システムおよびセンサ情報、電源管理機能、エラーイベントログにアクセスすることができます。さらに、テキストコンソールリダイレクションまたは SMASH CLP シェルを開始できます。SSH（Secure Shell）を使用してリモートマネージャを呼び出した場合、リモートマネージャと管理対象サーバの間の接続は暗号化されます。

  リモートマネージャを使用した iRMC S4 の操作については、303 ページ の「Telnet/SSH 経由の iRMC S4 (リモートマネージャ)」の章を参照してください。

- **リモートマネージャ（シリアル）: シリアル 1 を使用したテキストベースのシリアルインターフェース**

  リモートマネージャ（シリアル）インターフェースは、リモートマネージャインターフェースと同じです。

1.4 iRMC S4 で使用される通信プロトコル

iRMC S4 通信プロトコルとポートを、表 1 に示します。

接続のリモート側	通信方向	接続の iRMC S4 側（ポート番号 / プロトコル）
RMCP	→	623/UDP
	←	623/UDP
HTTP ポート	→	80/TCP
	←	80/TCP
HTTPs ポート	→	443/TCP
	←	443/TCP
Telnet	→	3172/TCP
	←	3172/TCP
SSH	→	22/TCP
	←	22/TCP
トラップ	→	162/UDP
Email	→	25/TCP
	←	25/TCP
VNC ポート		
標準ポート	→	80/TCP
	←	80/TCP
セキュアポート	→	443/TCP
	←	443/TCP

表 1: iRMC S4 で使用される通信プロトコルとポート

1.5 IPMI - 技術的背景

iRMC S4 は、IPMI インターフェースを使用して BMC の機能を使用できるようにします。

インテリジェントプラットフォーム

「インテリジェントプラットフォーム管理」イニシアチブは、最近のサーバシステムの増しつつある複雑さに応えるものです。これらのサーバシステムを監視するための新しいソリューションを開発するために、いくつかのメーカーがこのイニシアチブに参加しています。

「インテリジェントプラットフォーム管理」という用語は、ソリューション（システムの監視およびリカバリのための機能をプラットフォーム管理のためのハードウェアおよびファームウェアに直接実装する）へのアプローチの核心となる面を表しています。

目標

目標は、プラットフォーム管理用に中央システムコントローラ（Baseboard Management Controller - BMC) とインテリジェントプラットフォーム管理ハードウェアの間で標準化された抽象的なメッセージベースのインターフェースを定義することでした。

この標準化委員会は、さまざまなプラットフォーム管理モジュールの中心的特質を標準化された記述にまとめました。

定義

IPMI の仕様では、次のように定義されています。

「IPMI は、' 管理ソフトフェアで中立的な存在 ' であるハードウェアレベルのインターフェースの仕様であり、DMI、WMI、CIM、SNMP などの標準的な管理ソフトウェアインターフェースを通じて公開できる監視および制御機能を提供する。また、ハードウェアレベルのインターフェースとして、一般的な管理ソフトウェアスタックの下部に存在する」[23 ページ の「IPMI と他の管理標準」 を参照]。

利点

IPMI の仕様では、システムのプロセッサ、BIOS、およびオペレーティングシステムのインベントリ、ログ、リカバリおよび監視のための機能の独立性が確保されています。

これは、システムがシャットダウンされ、電源がオフにされたときも、システムをプラットフォーム管理の対象にすることができることを意味します。

IPMI と他の管理標準

IPMI は、関連するオペレーティングシステムの下で動作しているシステム管理ソフトウェアと連携する形で最も効果的に使用されます。IPMI の機能の、管理アプリケーションおよびオペレーティングシステムによって提供される管理機能への統合により、強力なプラットフォーム管理環境が実現されます。

IPMI と管理ソフトウェアスタックの関係の概要を 図 2 に示します。

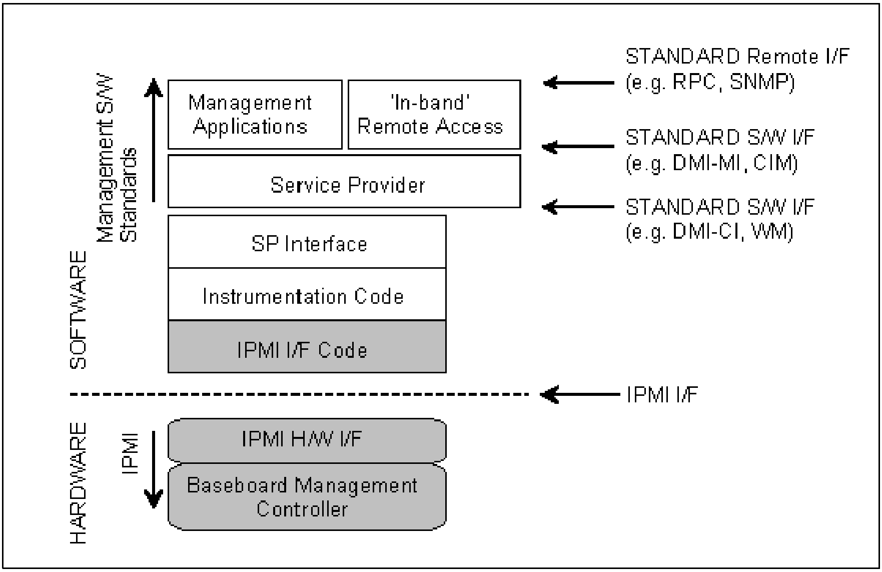


図 2: 管理ソフトウェアスタックでの IPMI（ソース : IPMI 仕様。30 ページ の「参照先」を参照してください。）

IPMI、IPMB および ICMB

IPMI イニシアチブは 3 つの主要な標準を生み出しました。

– *IPMI。インテリジェントプラットフォーム管理インターフェース（IPMI）仕様*では、より高いレベルのアーキテクチャ、つまり、IPMI ベースのシステムで使用される現在のコマンド、イベントフォーマット、データパケット、およびプロパティについて説明しています。

– *IPMB。インテリジェントプラットフォーム管理バス（IPMB）*は、I^2C ベース（書き込み専用）のバスであり、共通ハウジング内のさまざまなモジュール間の標準化された接続を提供します。
IPMB は、リモート管理モジュールの標準化されたインターフェースとしても使用することができます。

– *ICMB。インテリジェントシャーシ管理バス（ICMB）*（現在、ServerView Remote Management 環境には実装されていません。）は、プラットフォーム管理情報のやり取りおよび複数のシステムにわたる制御のための標準化されたインターフェースを提供します。ICMB は、IPMB に接続されるデバイスを使用して実装できるように設計されています。

IPMI の実装

IPMI の実装のコア要素は Baseboard Management Controller（BMC）です。BMC は以下のタスクを実行します。

– BMC は、システム管理ソフトウェアとプラットフォーム管理ハードウェアの間のインターフェースを編成します。

– また、監視、イベントログ、リカバリ制御のための自律的な機能を提供します。

– BMC は、システム管理ソフトウェアと IPMB の間のゲートウェイとしての役目を果たします。

IPMI では、追加の管理コントローラを、IPMB を使用して接続できるように、プラットフォーム管理を拡張できます。IPMB は、I^2C ベースのシリアルバスであり、システムのメインモジュール間で動作します。IPMB は、管理コントローラとの通信および管理コントローラ間の通信に使用されます。

複数の管理コントローラがサポートされている場合、IPMI はスケーラブルなアーキテクチャを提供します。つまり、複合サーバシステムでは、異なるサブシステム（たとえば、電源、ホットスワップ RAID ドライブモジュールなど）を監視するために複数のコントローラを使用できます。

また、IPMI は、「ローレベル」の I^2C コマンドを提供します。これには、IPMI のコマンドで処理できない「非インテリジェント」な I^2C モジュールで IPMB に接続されている管理コントローラを介してアクセスできます。

IPMI の実装の基本的な要素の概要は、26 ページ の図 3 を参照してください。

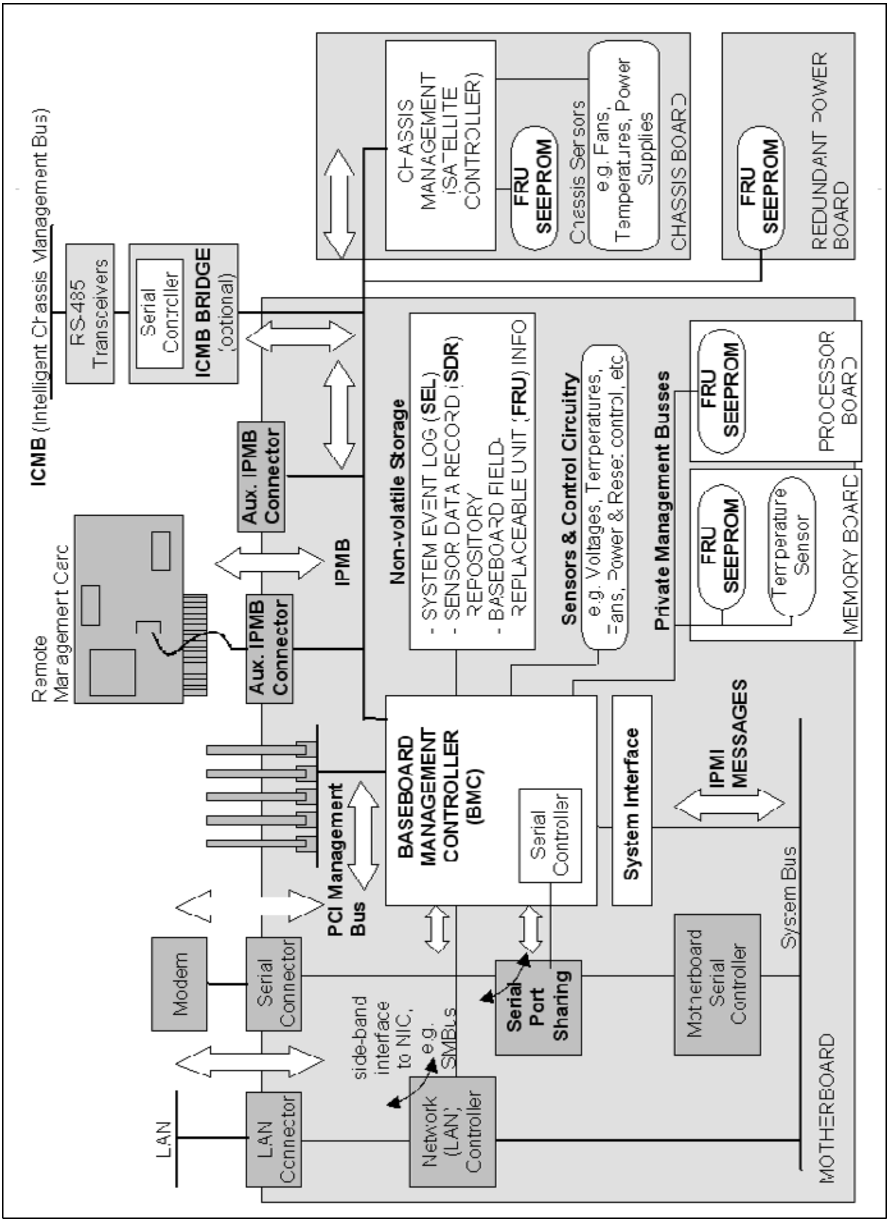


図 3: IPMI ブロック図（ソース : IPMI の仕様。次の節を参照してください :
30 ページ の「参照先」:

IPMI と「帯域内」/「帯域外」管理

システム管理の分野では、「帯域内」管理と「帯域外」管理は区別されます。

– 「帯域内」管理という用語は、管理対象サーバでオペレーティングシステムが実行されている場合に使用されます。

– 「帯域外」管理という用語は、管理対象サーバでオペレーティングシステムが実行されていない場合、たとえばハードウェアが故障している場合に使用されます。

IPMI 互換のシステムを持つ環境では、異なるインターフェースが使用できるため、IPMI 互換のシステムを「帯域内」でも「帯域外」でも管理できます。

IPMI-over-LAN

「IPMI-over-LAN」は、IPMI 標準での LAN インターフェースの仕様を表す現在の名前です。この仕様は、IPMI メッセージを管理対象システムの BMC との間で送受信できる方法を定め、メッセージは、RMCP (Remote Management Control Protocol) データパケットでカプセル化できます。これらの RMCP データパケットは IPv4（Internet Protocol Version 4）の UDP（User Datagram Protocol）を使用して Ethernet LAN 接続で転送されます。

RMCP プロトコルは、オペレーティングシステムが実行されていないときのシステムのステータスの管理をサポートするように指定されています。RMCP は簡単な照会 / 応答プロトコルです。

このような接続のインターフェースは、BMC に割り当てられているオンボード LAN コントローラで提供されます。

i このインターフェースは、挿入された LAN カードではなくオンボード LAN コントローラによってのみ提供できます。

RCMP が UDP の下で使用する 2 つのポートのうち、BMC は、ポート 623（プライマリ RMCP ポート）を使用して LAN コントローラと通信します。

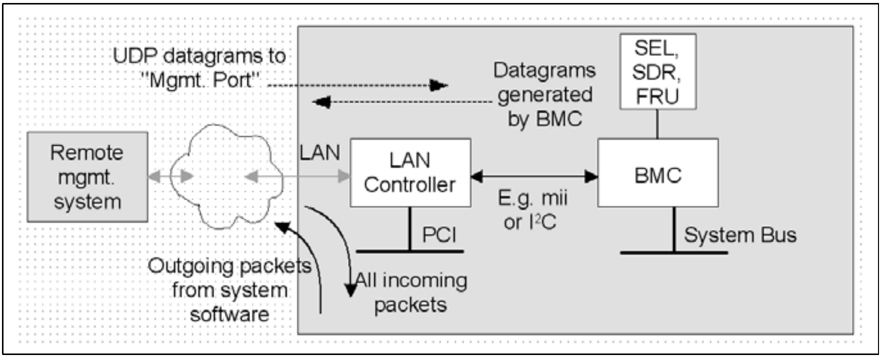


図 4: BMC と LAN コントローラ

Serial Over LAN インターフェース（SOL）

「Serial Over LAN」は、IPMI V2.0 規格に準拠しているインターフェースであり、LAN 接続上でのシリアルデータ転送を制御します。特に、SOL は、管理対象コンピュータとリモートワークステーションのシリアルコントローラの間の LAN 上でシリアルデータストリームを転送するためのパケットフォーマットおよびプロトコルを指定します。SOL は IPMI-over-LAN 仕様に基づいています。

SOL 接続を確立するために。リモート管理アプリケーションはまず、BMC との IPMI-over-LAN セッションを開始します。これが完了したら、リモートワークステーションから SOL サービスを有効にすることができます。シリアルコントローラとリモートワークステーションの間のデータトラフィックは、IPMI のコマンドと同じ IPMI セッション上で処理されます。

SOL 接続が確立されるとすぐに、シリアルコントローラとリモートワークステーションの間のデータ転送が以下のように実行されます。

– シリアルコントローラからリモートワークステーションへの転送 :
  シリアルコントローラによって発行されるデータストリームが BMC によってパーティション化され、パッケージ化されて、LAN 上でリモートワークステーションに送信されます。

– リモートワークステーションからシリアルコントローラへの転送 :
  BMC は、リモートワークステーションによって送信されたパッケージに含まれる文字をアンパックし、文字ストリームとしてシリアルコントローラに転送します。

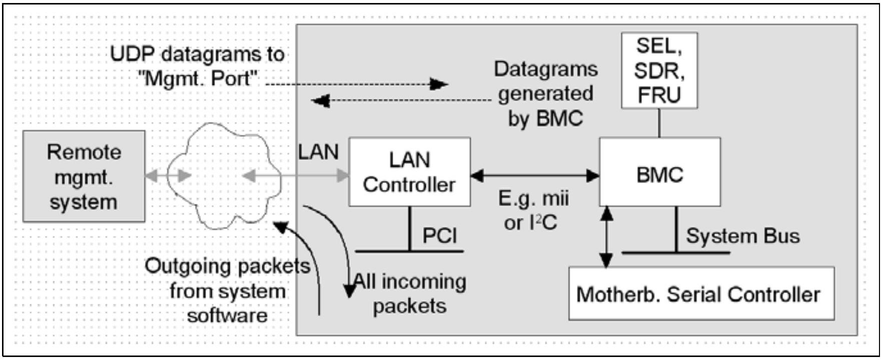


図 5: BMC と SOL

SOL 文字データが、SOL メッセージとして管理対象システムの BMC とリモートワークステーションの間でやり取りされます。SOL メッセージが RMCP+ データパケットにカプセル化され、IPv4（Internet Protocol Version 4）を使用した Ethernet LAN 接続上で UDP データグラム形式で転送されます。RMCP+ プロトコルは、RMCP プロトコルに基づいていますが、暗号化、認証などの仕様拡張が含まれています。

Serial over LAN は、管理対象サーバの BIOS とオペレーティングシステムの両方でのコンソールリダイレクションによる「ヘッドレス」管理を可能にしています。高コストな集線装置ソリューションは必要ありません。

IPMI でのチャネルのコンセプト

「チャネル」は、IPMI メッセージがさまざまな接続キャリアを介して BMC にルーティングされるときに使用される仕組みを提供します。最大 9 つのチャネルをサポートできます。システムインターフェースと IPMB は固定されています。他の 7 つのチャネルは実装に使用できます。

チャネルは「セッションベース」か「セッションレス」のどちらかにすることができます。「セッション」というコンセプトには 2 つの意味があります。ユーザ認証（30 ページ の「ユーザ ID」）を行うコンセプトと、単一のチャネルを使用した複数の IPMI メッセージストリームをルーティングするコンセプトです。

「セッションベース」チャネルの例には、LAN チャネルまたはシリアル / モデムチャネルがあります。「セッションレス」チャネルの例には、システムインターフェースおよび IPMB があります。

ユーザ ID

「セッションベース」チャネル（29 ページ の「IPMI でのチャネルのコンセプト」を参照）の場合、ユーザログインが必要です。一方、「セッションレス」チャネルには、ユーザ認証はありません。

IPMI の下で、ユーザ設定はチャネル固有です。したがって、ユーザは BMC に LAN チャネル経由でアクセスしているか、シリアルチャネル経由でアクセスしているかに応じて、異なる権限を持つことができます。

参照先

IPMI 標準に関する情報は、インターネットの以下のサイトを参照してください。

http://developer.intel.com/design/servers/ipmi/index.htm

1.6 DCMI（データセンター管理インターフェース）

iRMC S4 は DCMI（データセンター管理インターフェース）プロトコルをサポートしており、これは IPMI V2.0 規格に準拠しています。DCMI は、大規模データセンターに展開されたサーバシステムの管理と効率を向上させるために開発されました。

データセンター内のサーバのハードウェア管理要件を満たすため、DCMI は特に次の主要機能をサポートします。

– インベントリ機能（サーバ識別）
– 電源管理と消費電力監視
– 電力消費の監視と管理
– イベントログ
– 温度監視

DCMI の詳細情報は、DCMI ホームページに掲載されています。

http://www.intel.com/technology/product/DCMI

1.7 ServerView Suite リンク集

リンク集により、富士通は ServerView Suite および PRIMERGY サーバに関するさまざまなダウンロードや詳細情報を提供します。

ServerView Suite には、以下のトピックに関するリンクがあります。

- サポートデスク
- マニュアル
- 製品情報
- セキュリティ情報
- ソフトウェアのダウンロード

PRIMERGY サーバには、以下のトピックに関するリンクがあります。

ダウンロードには以下が含まれます。

- ServerView Suite の現在のソフトウェアバージョンおよびその他の Readme ファイル。
- ServerView Update Manager により PRIMERGY サーバをアップデートする場合、および ServerView Update Manager Express により個々のサーバをローカルでアップデートする場合の、システムソフトウェアコンポーネントの情報ファイルおよびアップデートセット。
- ServerView Suite のすべてのドキュメントの最新バージョン。

ダウンロードは富士通 Web サーバから無償で入手できます。

- サポートデスク
- マニュアル
- 製品情報
- スペアカタログ

リンク集へのアクセス

ServerView Suite のリンク集へアクセスする方法はいくつかあります。

1. ServerView Operations Manager から。

   ► 開始ページまたはメニューバーで「*ヘルプ*」–「*リンク*」を選択します。

   ServerView リンク集の開始ページが開きます。

2. 富士通マニュアルサーバで ServerView Suite のオンラインドキュメントの開始ページを使用する。

   i 次のリンクを使用して、オンラインドキュメントの開始ページにアクセスします。

   http://manuals.ts.fujitsu.com

   ► 左側の選択リストで「*Industry standard servers*」を選択します。

   ► メニュー項目「*PRIMERGY ServerView Links*」をクリックします。

   ServerView リンク集の開始ページが開きます。

3. ServerView Suite DVD から

   ► PRIMERGY ServerView Suite DVD の開始ウィンドウで、「*Select ServerView Software Products*」を選択します。

   ► 「*Start*」をクリックします。ServerView Suite のソフトウェア製品が表示されるページが開きます。

   ► メニューバーで「*LINKS*」を選択します。

   ServerView リンク集の開始ページが開きます。

1.8 ServerView Suite のマニュアル

ServerView Suite のマニュアルは、インターネットからも無料でダウンロードできます。オンラインマニュアルは、*http://manuals.ts.fujitsu.com* の *Industry standard servers* のリンク先からダウンロードできます。

1.9 表記規約

このマニュアルで使用している記号の意味は以下のとおりです。

警告	この記号は、身体の危険を表すか、データ喪失またはハードウェア破損につながりうるリスクへの注意を喚起するために使用しています。
	この記号は、重要な情報やヒントを強調するために使用しています。
►	この記号は、実行する必要があるアクションを示します。
斜体のテキスト	文中のコマンド、メニュー項目、ボタン名、オプション、ファイル名、およびパスは、*斜体*で示します。
< テキスト >	実際の値に置き換える必要のある変数を示します。
固定幅フォント	システムからの出力は、固定服フォントで示します。
固定幅フォント **ボールド固定幅フォント**	キーボードで入力する必要があるコマンドは、ボールド固定幅フォントで示します。
[角括弧]	入力は必須ではないことを示します。
{ 中括弧 }	「|」で区切って選択肢のリストを示します。
[キーボード] [記号]	キーは、キーボードに表示されているとおりに示します。大文字での入力を明示的に示す場合は、Shift キーを併記します（例 : A の場合、[SHIFT] - [A]）。 2 つのキーを同時に押す場合は、2 つのキーをハイフンで連結して示します。

表 2: 表記規約

このマニュアル内のテキストへの参照は、章または項の見出しと、章または項の開始ページで示します。

2 iRMC S4 への初回ログオン

iRMC S4 の工場出荷時のデフォルト設定を使用して、設定作業を一切行わずに iRMC S4 に初回ログインできます。

2.1 要件

リモートワークステーション :

– Windows：Internet Explorer バージョン 10.x 以降。
  Linux：Mozilla Firefox 3.x。

– コンソールリダイレクションの場合 :
  Sun Java Virtual Machine バージョン 1.6 以降。

ネットワーク内

– ネットワークに DHCP サーバが必要です。

– IP アドレスの代わりに具体的な名前を使用して iRMC S4 Web インターフェースにログインする場合、ネットワークの DHCP サーバを動的 DNS に設定する必要があります。

– DNS を設定する必要があります。設定しない場合は、IP アドレスを要求する必要があります。

2.2 iRMC S4 の工場出荷時のデフォルト

iRMC S4 のファームウェアには、デフォルトの 管理者 ID と iRMC S4 のデフォルトの DCHP 名が用意されています。

デフォルトの 管理者 ID :

管理者 ID :	admin
パスワード :	admin

管理者 ID とパスワードは、大文字小文字を区別します。

セキュリティ上の理由から、一度ログインした後は、新しい管理者アカウントを作成してデフォルトの管理者アカウントを削除するか、少なくともパスワードを変更するようにお勧めします（252 ページ の「ユーザ管理」の項を参照）。

iRMC S4 のデフォルト DHCP 名

iRMC S4 のデフォルトの DCHP 名は次の形式です :
IRMC< シリアル番号 >

シリアル番号は、iRMC S4 の MAC アドレスの最後の 3 バイトです。iRMC S4 の MAC アドレスは、PRIMERGY サーバのラベルに記載されています。

ログイン後、iRMC S4 の MAC アドレスは、「*ネットワークインターフェース*」ページ（230 ページを参照）のフィールドに読み取り専用エントリとして表示されます。

2.3 iRMC S4 Web インターフェースへのログイン

▶ リモートワークステーションから Web ブラウザを開いて、iRMC S4 の DNS 名または IP アドレスを入力します。

> **i** iRMC S4 の DNS 名は、PRIMERGY サーバのラベルに記載されています。

次のログインプロンプトが表示されます。

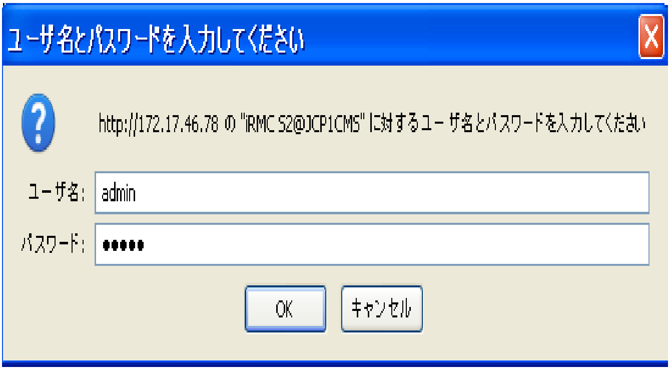


図 6: iRMC S4 Web インターフェースのログインプロンプト

> **i** ログインプロンプトが表示されない場合は、LAN 接続を確認してください（43 ページ の「LAN インターフェースのテスト」の項を参照）。

▶ デフォルトの管理者アカウントのデータを入力してください。

ユーザ名 : admin

パスワード : admin

▶「*OK*」をクリックして、入力を確定してください。

iRMC S4 Web インターフェースが開き、「*システム情報*」ページ（131 ページを参照）が表示されます。

3 iRMC S4 の設定

iRMC S4 の設定には、以下のツールが使用できます。

– UEFI セットアップユーティリティ（42 ページを参照）
– iRMC S4 Web インターフェース（119 ページを参照）
– Server Configuration Manager（333 ページ を参照）

この章では次の点について説明します。

– UEFI セットアップユーティリティを使用した iRMC S4 の LAN インターフェースの設定（42 ページを参照）。
– UEFI セットアップユーティリティを使用した LAN 経由のテキストコンソールリダイレクションの設定（44 ページを参照）。
– UEFI セットアップユーティリティを使用した iRMC S4 のシリアルインターフェースの設定（49 ページ）。
– Web インターフェースを使用した iRMC S4 の設定（52 ページ）。

3.1 iRMC S4 の LAN インターフェースの設定

この節では以下について説明します。

– LAN インターフェースの設定の要件
– UEFI セットアップユーティリティの LAN インターフェースの設定
– LAN インターフェースのテスト

i iRMC S4 接続の「スパニングツリー」のツリーは、無効にしておきます。（例：Port Fast=enabled; Fast Forwarding=enabled）。

3.1.1 前提条件

IP アドレスの設定に関しては、次の要件に注意する必要があります。

– LAN ケーブルが正しいポートに接続されていること。(40 ページ の「正しい LAN ポートへの接続」の項を参照)。

– iRMC S4 とシステムの IP アドレス間の相互動作(41 ページ の「iRMC S4 とシステムの IP アドレス間の相互動作」の項を参照)。

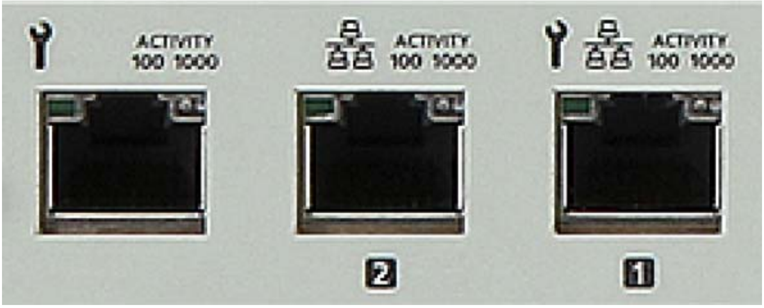
3.1.1.1 正しい LAN ポートへの接続

LAN 接続インターフェースは、iRMC iRMC S4 に割り当てられたオンボード LAN コントローラ上にあります（28 ページ の図 4 を参照）。

サーバタイプによって、PRIMERGY サーバには、システムボードの LAN インターフェースが 2 つのものと 3 つのものとがあります。レンチ記号がついているポートが、iRMC S4 用ポートです（例：図 7 のポート 1 および左上のポート）。

i LAN ケーブルが正しいポートに接続されていることを確認してください。

レンチ記号がついているポートは、PRIMERGY サーバのタイプによって異なることがあります。



Dedicated Service / Management LAN
（iRMC S4 用専用ポート。
iRMC S4 では最大 1000MBit/s の LAN 速度が使用可能です。これはハードウェアによります。）

[1] 共用 LAN
（iRMC S4 およびシステム）

[2] LAN（システム専用ポート）

図 7: iRMC S4 用ポート（レンチ記号で示される箇所）

3.1.1.2 iRMC S4 とシステムの IP アドレス間の相互動作

（オペレーティングシステムではなく）iRMC S4 に確実にデータパケットを転送するために、PRIMERGY サーバの LAN コントローラには、iRMC S4 専用の IP アドレスが必要です。

iRMC S4 の IP アドレスは、システム（オペレーティングシステム）とは別でなければなりません。

3.1.1.3 他のサブネットからのアクセス

リモートワークステーションが、DHCP を使用しないで管理対象サーバの iRMC S4 に別サブネットからアクセスする場合、ゲートウェイを設定する必要があります。

3.1.2 LAN インターフェースの設定：Configuration Tools

iRMC S4 の LAN インターフェースの設定には、いくつかの方法があります。

PRIMERGY サーバの機種によって、設定方法が異なります。

– UEFI セットアップユーティリティを使用する（42 ページを参照）

– iRMC S4 Web インターフェースを使用する（229 ページ の「ネットワーク設定 - LAN パラメータの編集」の項を参照）

– Server Configuration Manager を使用する（333 ページ の「Server Configuration Manager を使用した iRMC S4 の設定」の章 を参照）。

3.1.3 UEFI セットアップユーティリティを使用した LAN インターフェースの設定

iRMC S4 の LAN インターフェースを、UEFI セットアップユーティリティを使用して設定できます。

► 管理対象サーバの UEFI セットアップユーティリティを呼び出します。
サーバの起動中に [F2] を押します。

► 「*iRMC LAN parameter configuration*」メニューを呼び出します。

「*Server Mgmt*」–「*iRMC LAN Parameters Configuration*」

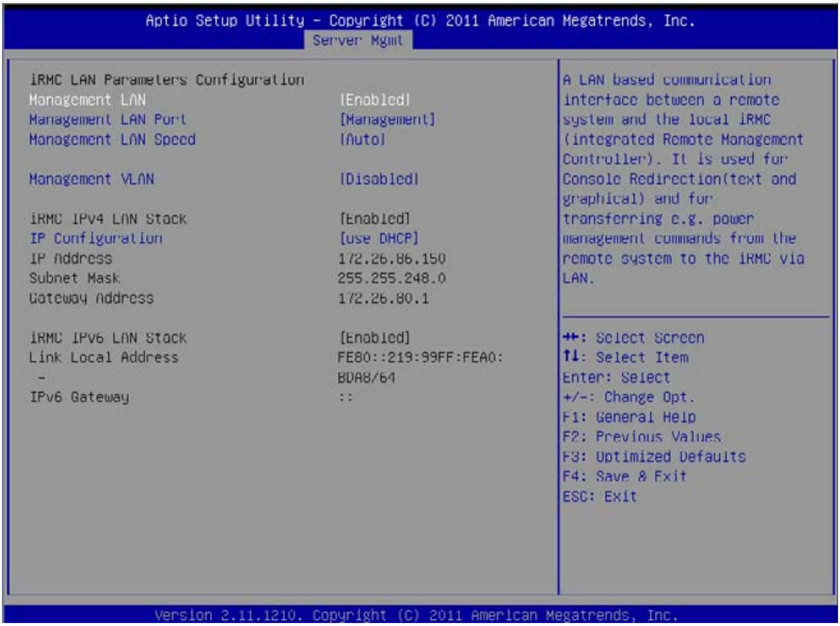


図 8: 「iRMC LAN Parameters Configuration」メニュー

► 以下の設定を行います。

Management LAN

値を「*Enabled*」に設定します。

Management LAN Port

「*Management*」設定を推奨します。

i 残りの設定の指定方法については、229 ページ の「ネットワーク設定 - LAN パラメータの編集」の項を参照するか、またはお使いのサーバの『BIOS (Aptio) Setup Utility』マニュアルを参照してください。

- ▶ 設定を保存します。
- ▶ iRMC S4 でコンソールリダイレクションを使用する場合は、45 ページ の「iRMC S4 のテキストコンソールリダイレクションの設定」の項に進みます。

  iRMC S4 でテキストコンソールリダイレクションを使用しない場合は、UEFI セットアップを終了して、次の「LAN インターフェースのテスト」の項に進みます。

3.1.4 LAN インターフェースのテスト

次の手順で、LAN インターフェースをテストします。

- ▶ Web ブラウザから、iRMC S4 Web インターフェースにログインしてください。ログインプロンプトが表示されない場合には、LAN インターフェースが動作していない可能性があります。
- ▶ Ping コマンドで、iRMC S4 接続をテストしてください。

3.2 UEFI セットアップユーティリティを使用した LAN 経由のテキストコンソールリダイレクションの設定

テキストコンソールリダイレクション設定およびサーバのオペレーティングシステムにより、テキストコンソールリダイレクションは以下の使用方法があります。

– BIOS POST フェーズの間のみ使用できる。

– BIOS POST フェーズ終了後も、オペレーティングシステムが稼働している間は使用できる。

この節では以下について説明します。

– UEFI セットアップユーティリティを使用した LAN 経由のテキストコンソールリダイレクションの設定。

– オペレーティングシステムの稼働中にコンソールリダイレクションを使用する場合に考慮するべきオペレーティングシステムの特別な必要条件。

i iRMC S4 Web インターフェースからも LAN を通したテキストコンソールリダイレクションを設定できます（283 ページ の「BIOS テキストコンソール - テキストコンソールリダイレクションの設定と開始」の項を参照）。

3.2.1 iRMC S4 のテキストコンソールリダイレクションの設定

► 管理対象サーバの UEFI セットアップユーティリティを呼び出します。
サーバの起動中に [F2] を押します。

► 「*Server Mgmt*」メニューを呼び出します。

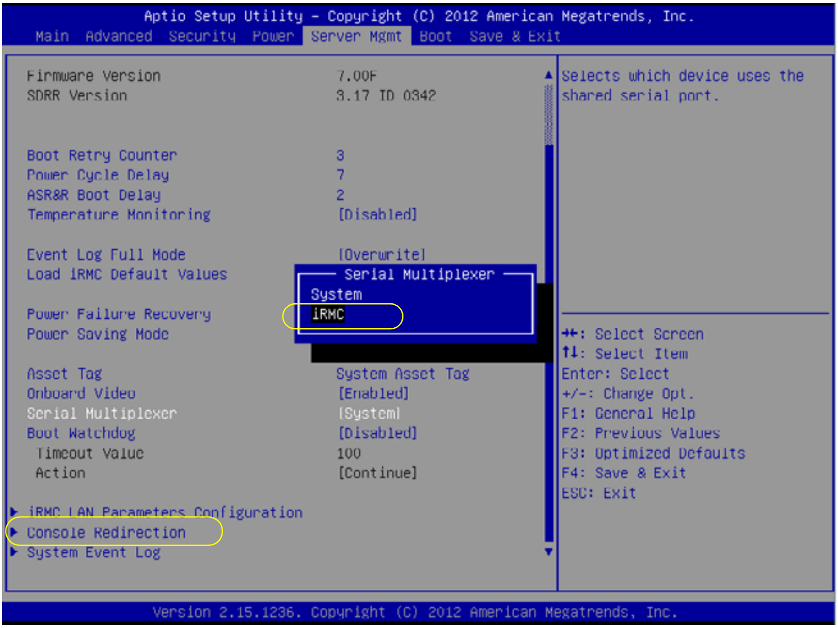


図 9: 「Server Mgmt」メニュー

► 以下の設定を行います。

Serial Multiplexer
　値を「*iRMC*」に設定します。

► 「*Console Redirection*」メニューを呼び出します。

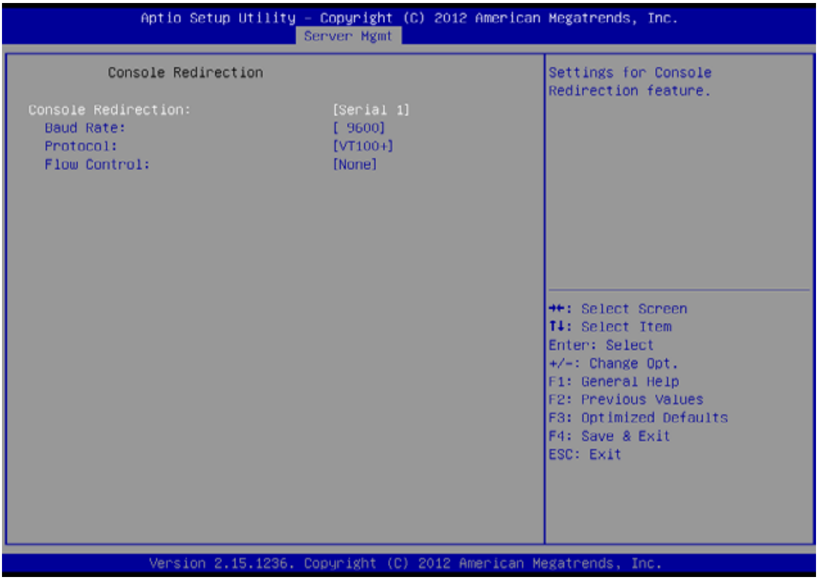


図 10: 「Console Redirection」メニュー

► 「*Console Redirection*」メニューで次の設定を行います。

Console Redirection

値を「*Serial 1*」に設定します。この場合、ターミナルは最初のシリアルインターフェースを使用します。

Baud Rate

ボーレートを指定します。

Protocol

この設定は変更しません（設定は使用するターミナルのタイプに依存します）。

Flow Control

設定は使用するターミナルのタイプに依存します。設定は、ターミナルと管理対象サーバで同一にする必要があります。

UEFI セットアップユーティリティの終了

► 設定を保存して、UEFI セットアップユーティリティを終了します。

► 43 ページ の「LAN インターフェースのテスト」の項に進みます。

3.2.2 オペレーティングシステム実行中のコンソールリダイレクションの使用

管理対象サーバのオペレーティングシステムによっては、BIOS POST フェーズ後もコンソールリダイレクションの使用を継続することができます。

Windows Server 2008/2012

Windows インストール中に有効にした場合は、コンソールリダイレクションは自動的に設定されます。

コンソールリダイレクションが Windows インストールの完了後に有効にされた場合は、コンソールリダイレクションを手動で設定する必要があります。

Windows Server 2008/2012 では、POST フェーズ後、自動的にコンソールリダイレクションを使用できます。さらに設定を行う必要はありません。オペレーティングシステムの起動中に、Windows Server SAC コンソールに切り替わります。

図 11: Windows Server SAC コンソール

Linux

Linux オペレーティングシステムでは、POST フェーズ後にコンソールリダイレクションを使用するために、次の設定を行う必要があります。一度設定すると、リモートワークステーションから無制限にアクセスできます。

必要な設定

設定は、プログラムのバージョンによって異なる場合があります。

SuSe および RedHat

/etc/inittab ファイルの最後に次の行を追加します。

xx:12345:respawn:/sbin/agetty <baud-rate> ttyS0

RedHat

/etc/grub.conf ファイルのカーネルブートパラメータに以下を追加します。

console=ttyS0,<baud-rate> console=tty0

SuSE

/boot/grub/menu.lst ファイルのカーネルブートパラメータに以下を追加します。

console=ttyS0,<baud-rate> console=tty0

3.3 iRMC S4 のシリアルインターフェースの設定と使用

iRMC S4 のシリアルインターフェースを使用すると、ヌルモデムケーブル経由でターミナルアプリケーションのリモートマネージャ（シリアル）を使用できます（51 ページ の「リモートマネージャ（シリアル）の使用」の項を参照）。

3.3.1 iRMC S4 を使用したシリアルインターフェースの設定

▶ 管理対象サーバの UEFI セットアップユーティリティを呼び出します。
サーバの起動中に [F2] を押します。

▶ 「*Server Mgmt*」メニューを呼び出します。

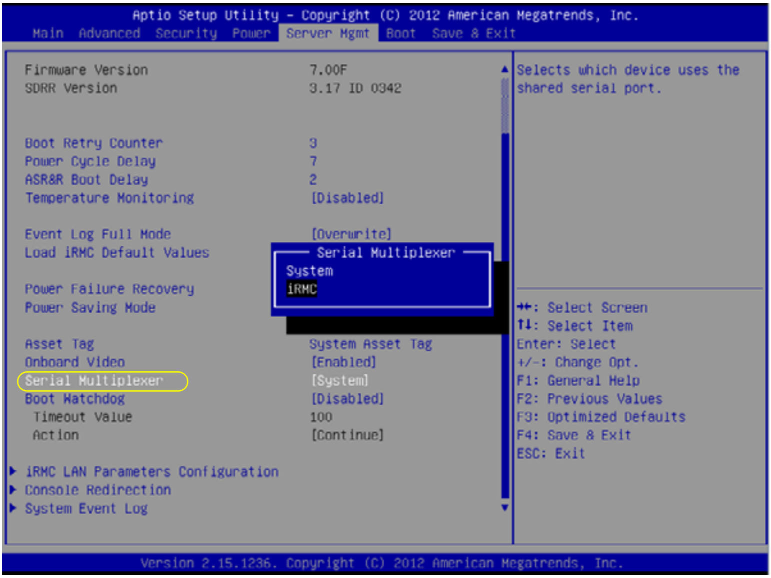


図 12: 「Server Mgmt」メニュー

▶ 以下の設定を行います。

Serial Multiplexer

値を「*iRMC*」に設定します。

► 「*Serial Port 1 Configuration*」メニューを呼び出して、シリアルポートを設定します。

「*Advanced*」–「*Super IO Configuration* 」「*Serial Port 1 Configuration*」:

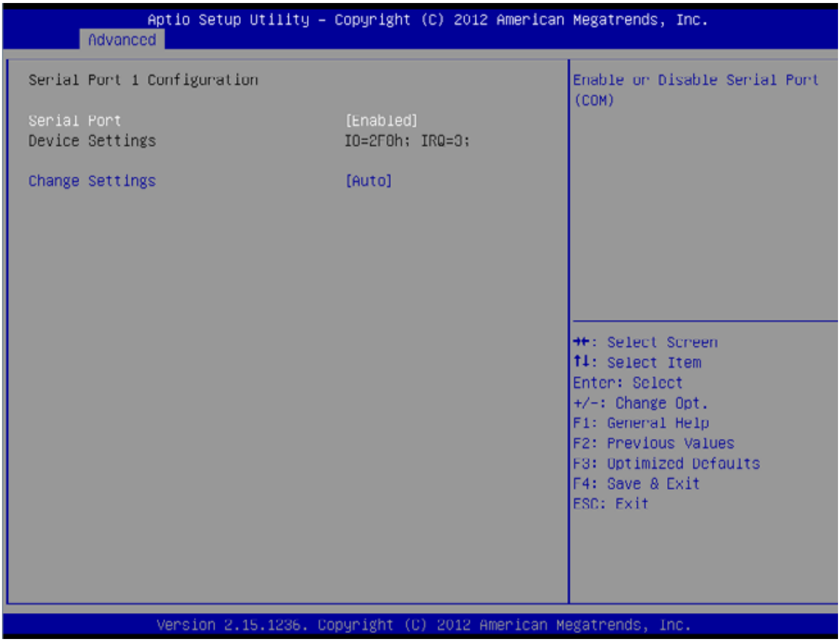


図 13: Serial Port 1 設定メニュー

► 以下の設定を行います。

Serial Port

値を「*Enabled*」に設定します。

Device Settings

ベース I/O アドレスと、対応するシリアルポートへのアクセスに使用される割り込みを表示します（IO=2F8h; IRQ=3 など）。

指定された値のペアを受理します。

UEFI セットアップユーティリティの終了

► 設定を保存して、UEFI セットアップユーティリティを終了します。

► 43 ページ の「LAN インターフェースのテスト」の項に進みます。

3.3.2 リモートマネージャ（シリアル）の使用

ヌルモデルケーブルでコンピュータを接続して、ターミナルプログラム（VT100+）をこのコンピュータで起動すると、リモートマネージャ（シリアル）ターミナルプログラムにアクセスできます。リモートマネージャ（シリアル）インターフェースは、リモートマネージャインターフェースと同じです（303 ページ の「Telnet/SSH 経由の iRMC S4 (リモートマネージャ)」の章 を参照）。

前提条件

管理対象サーバ :

iRMC 上の「*Serial Multiplexer* BIOS」を設定する必要があります（49 ページ の「iRMC S4 を使用したシリアルインターフェースの設定」の項を参照）。

ターミナルプログラム（VT100+）:

次のように、ターミナルプログラムのポートの設定を行います。

Bits per second

値を「*38400*」に設定します。

Data bits

値を「*8*」に設定します。

Parity

値を「*None*」に設定します。

Stop bits

値を「*1*」に設定します。

Flow Control

値を「*None*」に設定します。

3.4 iRMC S4 Web インターフェースによる iRMC S4 の設定

► iRMC S4 Web インターフェースを起動します（120 ページ の「iRMC S4 Web インターフェースへのログイン」の項を参照）。

3.4.1 LAN パラメータの構成

► ナビゲーション領域の「*ネットワーク設定*」をクリックします（229 ページ の「ネットワーク設定 - LAN パラメータの編集」の項を参照）。

LAN 設定の構成

► 「*ネットワークインターフェース*」ページで LAN の設定を行います。設定の詳細については、230 ページ の「Network Interface - iRMC S4 上の Ethernet 設定の編集」の項を参照してください。

ポートとネットワークサービスの設定

► 「*ポートとネットワークサービス*」ページでポートおよびネットワークサービスを設定します。設定の詳細については、237 ページ の「ポート番号とネットワークサービス - ポートとネットワークサービスの設定」の項を参照してください。

DHCP/DNS 設定（動的 DNS）

► 「*DNS 設定*」のページで DNS の設定を行います。設定の詳細については、240 ページ の「DNS 構成 - iRMC S4 の DNS の設定」の項を参照してください。

3.4.2 通知の設定

通知設定のページは、ナビゲーション領域の「*通知情報設定*」にまとめられています（244 ページ の「通知情報設定 - 警告通知の設定」の項を参照）。

SNMP による通知転送の設定

- ナビゲーション領域の「*SNMP トラップ*」をクリックします。「*SNMP トラップ*」ページが表示されます。
- SNMP トラップ転送の設定設定の詳細については、245 ページ の「SNMP トラップ送信設定 - SNMP トラップ通知の設定」の項を参照してください。

E-mail 通知の設定（E-mail による通知）

- ナビゲーション領域の「*Email*」をクリックします。「*Email 通知*」ページが表示されます。
- グローバル Email 構成設定の詳細については、246 ページ の「Email 設定 - Email 送信設定」の項を参照してください。

3.4.3 テキストコンソールリダイレクションの構成

- 「*BIOS テキストコンソール*」ウィンドウで、テキストコンソールのリダイレクションを設定します。設定の詳細については、283 ページ の「BIOS テキストコンソール - テキストコンソールリダイレクションの設定と開始」の項を参照してください。

4 iRMC S4 のユーザ管理

iRMC S4 によるユーザ管理には 2 種類の異なるユーザ ID を使用します。

– **ローカルユーザー ID** は iRMC S4 内部の不揮発性記憶装置に保存され、iRMC S4 のユーザインターフェース経由で管理されます。

– **グローバルユーザ ID** はディレクトリサービスの集中データストアに保存され、ディレクトリサービスのインターフェース経由で管理されます。

  グローバル iRMC S4 ユーザ管理では、現在以下のディレクトリサービスがサポートされます。

  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP
  – OpenDJ

本章では以下について説明します。

– iRMC S4 によるユーザ管理の概念
– ユーザ権限
– iRMC S4 上のローカルユーザー管理

i 個別のディレクトリサービスを使用するグローバルユーザー管理の詳細については、『ServerView でのユーザ管理』マニュアルを参照してください。

4.1 iRMC S4 によるユーザ管理の概念

iRMC S4 によるユーザ管理は、ローカルとグローバルのユーザ ID を並列に管理することができます。

ユーザがいずれかの iRMC S4 のインターフェースにログインするために入力する認証データ（ユーザ名、パスワード）を検証する際には、iRMC S4 は以下のように処理します（合わせて 57 ページ の図 14 も参照してください）。

1. iRMC S4 はユーザ名とパスワードを内部に保存されたユーザ ID と照合します。
   - ユーザは、iRMC S4 認証に成功すれば（ユーザ名とパスワードが有効）ログインすることができます。
   - 認証に失敗した場合には、iRMC S4 はステップ 2 の検証手順を継続します。
2. iRMC S4 はユーザ名とパスワードを使用して、LDAP 経由でディレクトリサービスの認証を受け、LDAP クエリによってユーザの権限を判断してユーザに iRMC S4 を操作する権限があるかどうかを確認します。

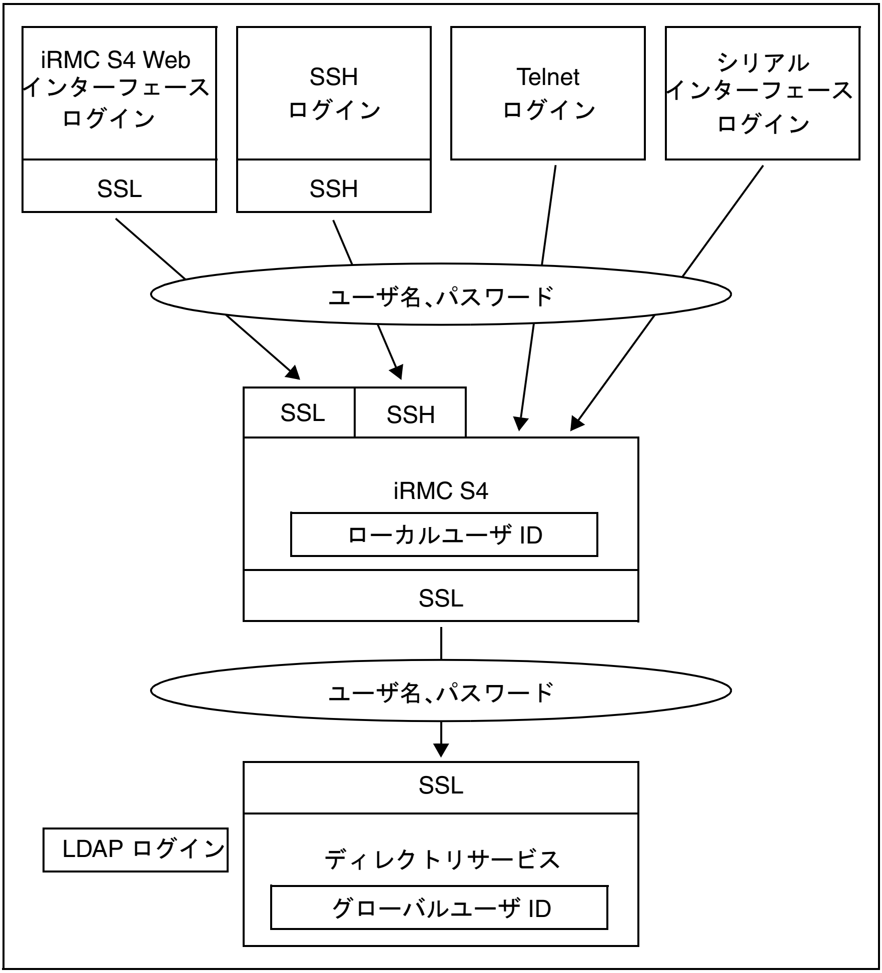


図 14: iRMC S4 経由のログイン認証

iRMC S4 とディレクトリサービスの間の LDAP 接続には、オプションの SSL を使用することを推奨します。SSL で保護された iRMC S4 とディレクトリサービスの間の LDAP 接続では安全なデータ交換が保証されますが、特にユーザ名とパスワードのデータの送信が安全にできます。

iRMC S4 Web インターフェース経由の SSL ログインが必要になるのは、LDAP が有効な場合のみです（「*LDAP 有効化*」オプション、263 ページを参照）。

4.2 ユーザ権限

iRMC S4 は以下の 2 つの相互補完的なユーザ権限を区別します。

– チャネル別の権限（チャネル別許可グループ割り当て）

– iRMC S4 独自の機能によるアクセス許可

i 個々の iRMC S4 機能を使用するために必要な特権と許可は次の通りです。

– iRMC S4 Web インターフェースについては、123 ページを参照

– リモートマネージャについては、313 ページを参照

チャネル別権限（チャンネル別許可グループ）

iRMC S4 は各々のユーザ ID を次の 4 つの チャンネル別許可グループのうちのいずれかに割り当てます。

– User
– Operator
– Administrator
– OEM

iRMC S4 はこれらの許可を、チャンネル固有を基本にして割り当てますので、ユーザは、iRMC S4 に LAN インターフェースを経由して接続したか、シリアルインターフェースを経由して接続したかにより、別々に許可を取得することができます。

与えられる許可の範囲は、「*User*」（最も低い許可レベル）から「*Operator*」、「*Administrator*」、「*OEM*」（最も高い許可レベル）の順に大きくなります。

i 許可グループは IPMI 権限レベルに対応しています。特定の許可（たとえば、「Power Management」）はこれらのグループまたは権限レベルに関連づけられます。

iRMC S4 独自の機能によるアクセス許可

チャネル別の許可に加えて、ユーザに次の許可を個別に割り当てることもできます。

– **ユーザアカウント変更権限**
  ローカルユーザ ID を設定する権限。

– **iRMC S4 設定変更権限**
  iRMC S4 設定を行う権限。

– **AVR 使用権限**
  「View Only」および「フルコントロール」モードで AVR（Advanced Video Redirection）を使用する権限

– **リモートストレージ使用権限**
  バーチャルメディア機能を使用する権限

初期設定のユーザ ID

iRMC S4 のファームウェアには、iRMC S4 用のすべての許可を持つデフォルトの管理者 ID が用意されています。

管理者 ID :	admin
パスワード :	admin

ローカルユーザの場合には管理者 ID もパスワードも大文字小文字を区別します。

最初にログインした時になるべく早く新しい管理者アカウントを作成して、デフォルトの管理者アカウントを削除するか、少なくともパスワードを変更しておくことを強く推奨します（252 ページ の「ユーザ管理」の項を参照）。

4.3 iRMC S4 のローカルユーザ管理

iRMC S4 には 固有のローカルユーザ管理方法があります。最大 16 人のユーザをパスワード付きで設定し、それぞれが属するユーザグループによってさまざまな権限を割り当てることができます。ユーザ ID は、iRMC S4 内部の不揮発性記憶装置に保存されます。

iRMC S4 のユーザ管理には次のオプションが使用可能です。

– Web インターフェースによるユーザ管理

– Server Configuration Manager によるユーザ管理

4.3.1 iRMC S4 Web インターフェースを使用したローカルユーザ管理

i iRMC S4 でのユーザ管理には「*ユーザ アカウント変更権限*」が必要です。

設定されたユーザのリストは Web インターフェースで表示できます。新しいユーザの設定、既存ユーザの設定変更、または、ユーザのリストからの削除が可能です。

▶ iRMC S4 Web インターフェースを起動します（120 ページ の「iRMC S4 Web インターフェースへのログイン」の項を参照）。

設定されたユーザのリスト表示

▶ ナビゲーション領域で「*ユーザ管理*」–「*iRMC S4 ユーザ管理*」をクリックします。

「*ユーザ管理*」ページが開いて設定されたユーザのリストが表示されます（253 ページを参照）。ここで、ユーザの削除と新しいユーザの設定ができます。
このページに関しては、252 ページ の「ユーザ管理」の項に説明があります。

新しいユーザの設定

▶ 「*ユーザ管理*」ページで、「*ユーザの新規作成*」ボタンをクリックします。

「*新規ユーザの構成*」ページが開きます。このページで新しいユーザの基本設定を設定することができます。このページに関しては、254 ページ の「新規ユーザの構成 - 新規ユーザの構成」の項に説明があります。

ユーザの設定変更

▶ 「*ユーザ管理*」ページで、設定されたパラメータを変更したいユーザのユーザ名をクリックします。

「*ユーザ 〈name〉 構成*」ページが開いて選択されたユーザの設定値を表示します。このページで新しいユーザの設定パラメータを変更することができます。このページに関しては、255 ページ の「「ユーザ “<name>” 構成」 - ユーザ設定（詳細）」の項に説明があります。

ユーザの削除

▶ 「*ユーザ管理*」ページで、削除するユーザと同じ行にある［*削除*］ボタンをクリックします。

4.3.2 Server Configuration Manager でのローカルユーザ管理

i **前提条件**：

管理対象サーバには最新の ServerView エージェントをインストールしておく必要があります。

i iRMC S4 でのユーザ管理には「*ユーザ アカウント変更権限*」が必要です。

Server Configuration Manager でのユーザ管理は、ほとんどの部分で iRMC S4 Web インターフェースを使用したユーザ管理と一致します。

Server Configuration Manager の起動方法の詳細は、333 ページ の「Server Configuration Manager を使用した iRMC S4 の設定」の章を参照してください。

個々の Configuration Manager ダイアログの詳細は、Server Configuration Manager のオンラインヘルプを参照してください。

4.3.3 iRMC S4 ユーザの SSHv2 公開鍵認証

ユーザ名とパスワードによる認証方法に加えて、iRMC S4 は SSHv2 に基づくローカルユーザの公開鍵と秘密鍵のペアを使用する公開鍵認証もサポートしています。SSHv2 公開鍵認証を実装するには、iRMC S4 ユーザの SSHv2 鍵を iRMC S4 にアップロードし、iRMC S4 ユーザは、たとえば、「*PuTTY*」プログラムまたは OpenSSH クライアントプログラムの「*ssh*」などでその秘密鍵を使用します。

iRMC S4 は以下の種類の公開鍵をサポートしています。

– SSH DSS（最低条件）
– SSH RSA（推奨）

iRMC S4 へアップロードする公開 SSHv2 鍵は、RFC4716 フォーマットでも OpenSSH フォーマットでも使用可能です（74 ページを参照）。

公開鍵認証

iRMC S4 の公開鍵認証は、おおむね以下のように処理されます。

iRMC S4 にログインするユーザが鍵のペアを作成します。

– 秘密鍵は読み取り保護され、ユーザのコンピュータ内に保存されます。

– ユーザ（または管理者）は公開鍵を iRMC S4 にアップロードします。

設定が正しければ、ユーザはパスワードの入力をしなくても非常に安全に iRMC S4 にログインすることができるようになります。ユーザの責任は秘密鍵の機密保護のみです。

秘密鍵の認証には以下の手続きが必要です。この手続きはこれ以降の節にも説明があります。

1. 「*PuTTYgen*」または「*ssh-keygen*」プログラムを使用して SSHv2 の公開鍵と秘密鍵を作成して、別々のファイルに保存します（63 ページを参照）。

2. SSHv2 鍵のファイルから iRMC S4 へのアップロード (67 ページを参照)。

3. 「*PuTTY*」または「*ssh*」プログラムを iRMC S4 への SSHv2 アクセス用に設定します（69 ページを参照）。

4.3.3.1 SSHv2 の公開鍵と秘密鍵の作成

SSHv2 の公開鍵と秘密鍵は以下の方法で作成することができます。

– プログラム「*PuTTYgen*」を使用する。

– または、OpenSSH クライアントプログラム、「*ssh-keygen*」を使用する。

PuTTYgen を使用する SSHv2 の公開鍵と秘密鍵の作成

次の手順に従います。

▶ ユーザの Windows コンピュータで *PuTTYgen* を起動します。

PuTTYgen が起動すると次の画面が表示されます。

図 15: PuTTYgen：SSHv2 の新しい公開鍵と秘密鍵の作成

▶ 「*Parameters*」の項目で *SSH-2RSA* 鍵タイプを選択し［*Generate*］をクリックすると鍵の生成が開始されます。

鍵生成の進行状況は「*Key*」の下部に表示されます（64 ページ の図 16 を参照）。

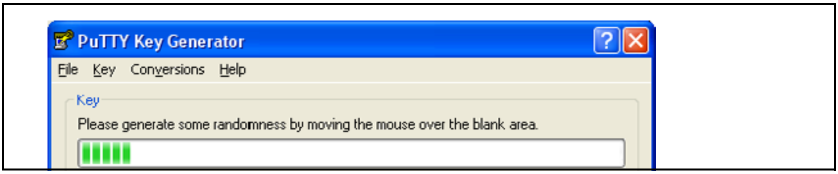


図 16: PuTTYgen：新しい鍵のペアの作成（プログレスバー）

► 進行表示部の空白部分でマウスポインタを動かすと、作成される鍵のランダム性がより増大します。

鍵が生成されると *PuTTYgen* が鍵と公開 SSHv2 鍵の指紋を表示します。

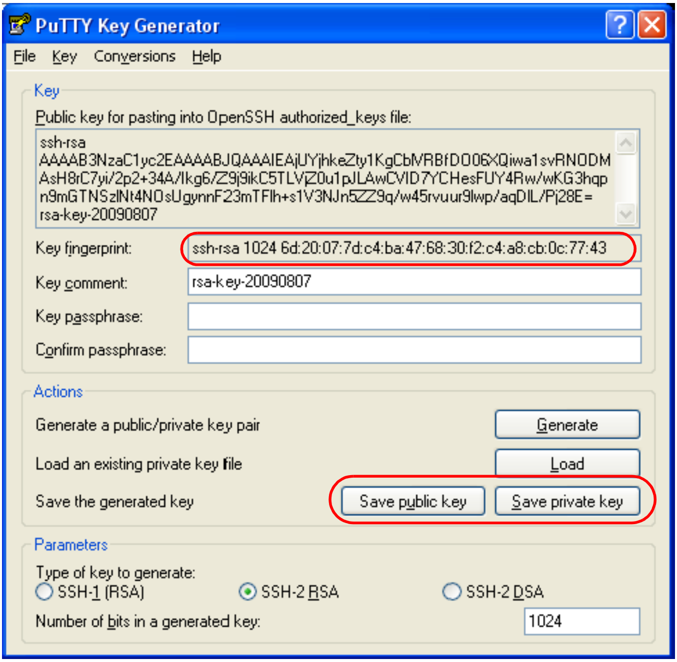


図 17: PuTTYgen：新しい秘密 SSHv2 鍵の作成（プログレスバー）

► ［*Save public key*］ボタンをクリックして、SSHv2 鍵をファイルに保存してください。このファイルから iRMC S4 に公開鍵をアップロードすることができます（67 ページを参照）。

► ［*Save private key*］をクリックして、*PuTTY* に使用する秘密 SSHv2 鍵を保存します（69 ページを参照）。

ssh-keygen を使用する SSHv2 の公開鍵と秘密鍵の作成

> **i** 使用している Linux の版にプリインストールされていない場合には、*http://www.openssh.org* から OpenSSH を入手できます。
>
> OpenSSH 用オペランドの詳しい説明は、*http://www.openssh.org/manual.html* で OpenSSH ユーザガイドを参照してください。

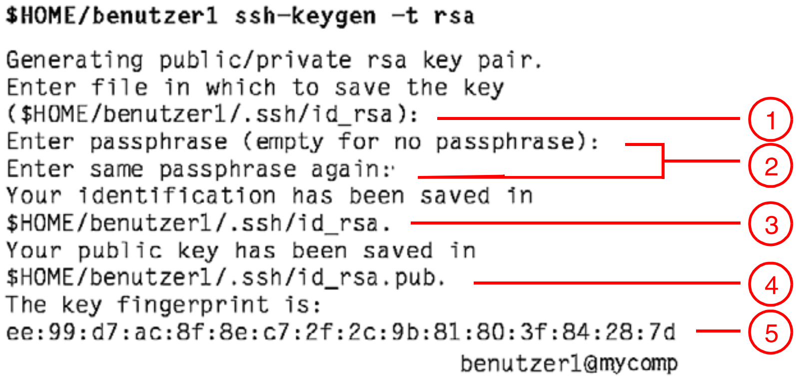
次の手順に従います。

► 「*ssh-keygen*」を呼び出して RSA 鍵のペアを生成させます。

```
ssh-keygen -t rsa
```

ssh-keygen は鍵生成処理の進行のログを作成します。*ssh-keygen* はユーザに秘密鍵を保存するファイル名と秘密鍵のパスフレーズを問い合わせます。*ssh-keygen* は生成された SSHv2 の秘密鍵と公開鍵を別々のファイルに保存し、公開鍵の指紋を表示します。

例：「ssh -keygen」による RSA 鍵ペアの生成



説明

1. 「*ssh-keygen*」は SSHv2 鍵を保存するファイル名を要求します。「[Enter]」が押下されてファイル名なしの入力が確認されると「*ssh-keygen*」はデフォルト名の「*id_rsa*」を使用します。
2. 「*ssh-keygen*」が秘密鍵の暗号化に使用するパスフレーズの入力（および確認）を要求します。[[Enter]] が押下されてパスフレーズなしの入力が確認されると、「*ssh-keygen*」はパスフレーズを使用しません。
3. 「*ssh-keygen*」は、新しく生成された秘密 SSHv2 鍵が「*/.ssh/id_rsa*」ファイルに保存されたことを知らせます。
4. 「*ssh-keygen*」は、新しく生成された公開 SSHv2 鍵が「*/.ssh/id_rsa.pub*」ファイルに保存されたことを知らせます。
5. 「*ssh-keygen*」は公開 SSHv2 鍵の指紋と公開鍵が属するローカルのログインを表示します。

4.3.3.2 SSHv2 鍵のファイルから iRMC S4 へのアップロード

次の手順に従います。

► iRMC S4 Web インターフェースで、「*iRMC S4 ユーザ管理*」ページの要求される一覧画面の詳細なビュー（この例では *user3*）を開きます。

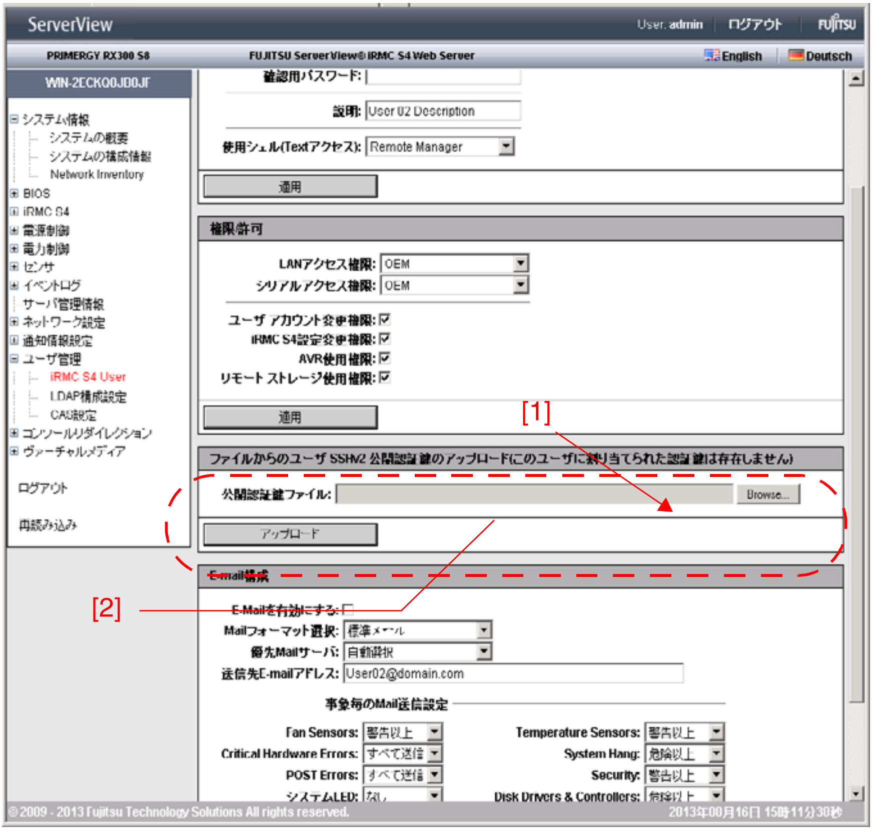


図 18: iRMC S4 Web インターフェース：公開 SSHv2 鍵の iRMC S4 へのアップロード

► 「*ファイルからのユーザ SSHv2 公開認証鍵のアップロード*」グループの中の［*参照*］ボタン（1）をクリックして、必要な公開鍵（2）のあるファイルまで進みます。

► 「*アップロード*」ボタンをクリックして公開鍵を iRMC S4 にアップロードします。

鍵が正常にアップロードされると、iRMC S4 は「*ファイルからのユーザ SSHv2 公開認証鍵アップロード*」グループの中に鍵の指紋を表示します。

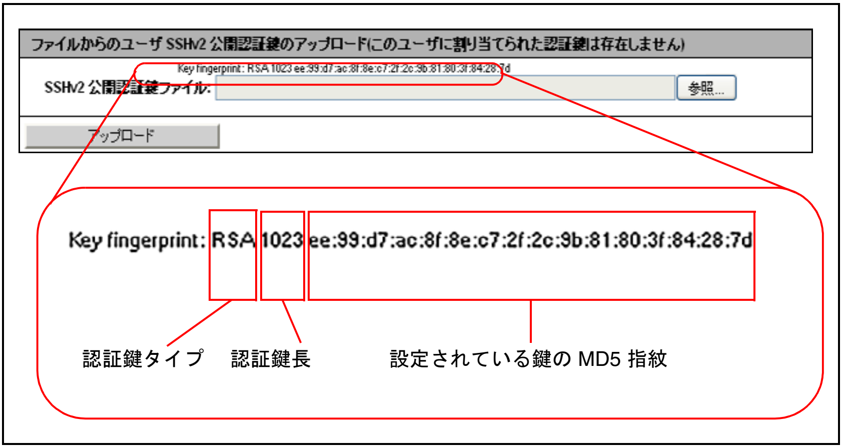


図 19: 鍵指紋の表示

i セキュリティのため、ここに表示された鍵指紋が *PuTTYgen* (64 ページ の図 17 を参照) の「*鍵指紋*」に表示された指紋と一致していることを確認してください。

4.3.3.3 PuTTY と OpenSSH クライアントが公開 SSHv2 鍵を使用するための設定

公開 SSHv2 鍵を使用する PuTTY の設定

PuTTY プログラムでは、iRMC S4 への公開鍵認証接続のセットアップと、自身のユーザ名または自動ログイン機能によるログインが可能になります。*PuTTY* は、事前に生成された公開／秘密 SSHv2 鍵のペアに基づいて、自動的に認証プロトコルを処理します。

次の手順に従います。

▶ ユーザの Windows コンピュータで *PuTTY* を起動します。

PuTTY が起動すると以下の画面が表示されます。

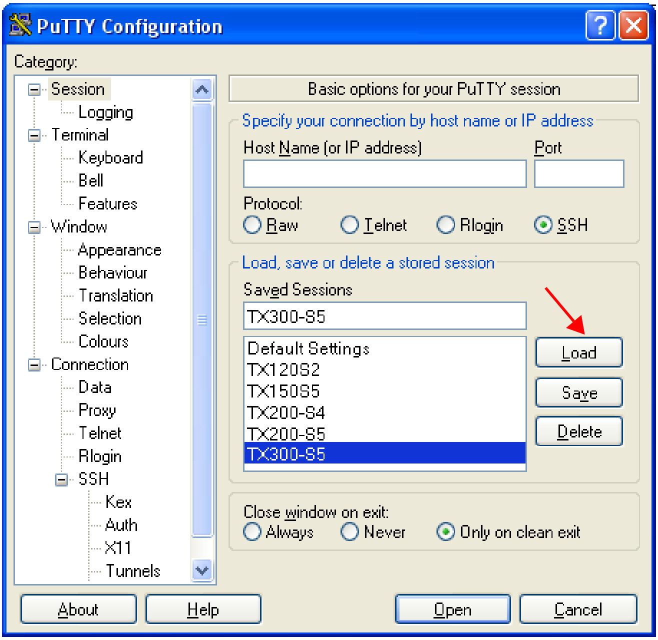


図 20: PuTTY：SSH セッションの選択とロード

▶ SSHv2 鍵を使用したい iRMC S4 に、保存されている SSH セッションを選択するか新しい SSH セッションを作成します。

► ［*Load*］をクリックして選択した SSH セッションをロードします。

その結果、次のウィンドウが開かれます。

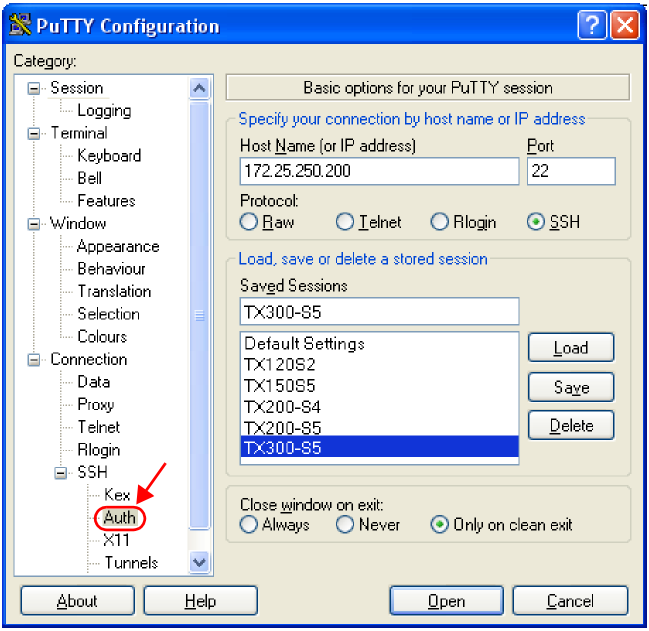


図 21: PuTTY：SSH セッションのロード

► 「*SSH - Auth*」を選択して、SSH 認証のオプションを設定します。

次のウィンドウが開きます（71 ページ の図 22 を参照）。

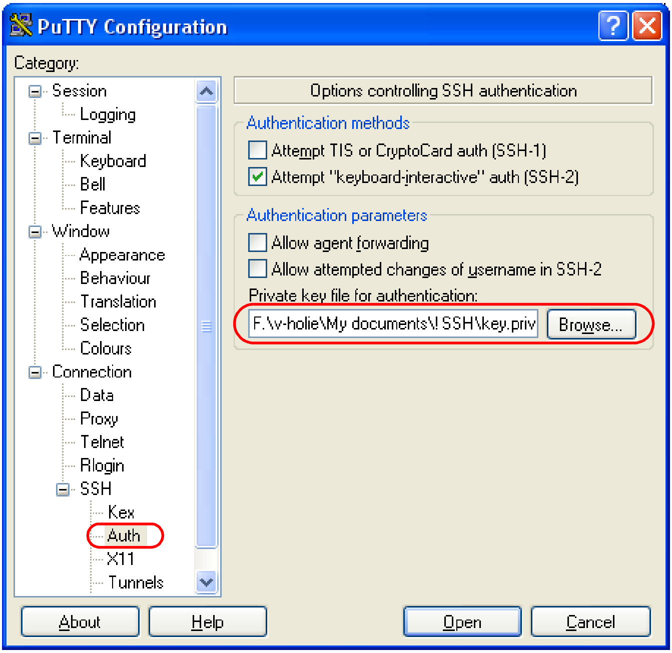


図 22: SSH 認証のオプションの設定

► iRMC S4 で使用する秘密鍵が入ったファイルを選択します。

> **i** **なお、次の点に注意してください。**
> この時点では必要なのは秘密鍵（64 ページを参照）であり、iRMC S4 にロードされた**公開鍵ではありません。**

i 「Connection」-「Data」で、iRMC S4 に自動ログインするユーザ名を追加指定できます。

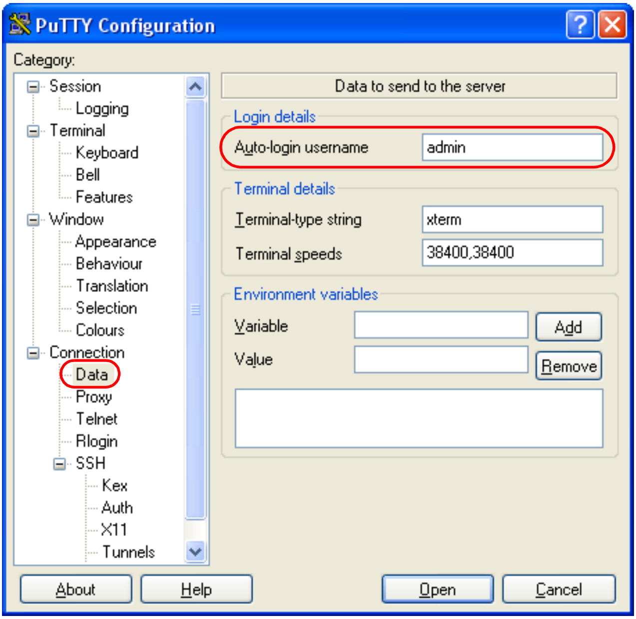


図 23: PuTTY：iRMC S4 に自動ログインするユーザ名の指定

公開 SSHv2 鍵に使用する OpenSSH クライアントプログラム ssh の設定

OpenSSH クライアントプログラム「*ssh*」を使用して SSHv2 で保護された iRMC S4 への接続を確立します。現在のローカルログインのままでも、別のログインでもログインすることができます。

i ログインは、iRMC S4 上のローカルログインとして設定され、関連する SSHv2 鍵は iRMC S4 にロードされていなければなりません。

「*ssh*」は以下のソースから順番に設定オプションを読み込みます。

1. 「*ssh*」を呼び出すときに使用したコマンドライン引数
2. ユーザ毎の設定ファイル（*$HOME/.ssh/config*）

   i このファイルにはセキュリティ上重要な情報は含まれていませんが、読取り／書込み許可はオーナーにしか付与しないでください。ほかのどのユーザに対しても、アクセスを拒否してください。

3. システム全体の設定ファイル（*/etc/ssh/ssh_config*）

以下の場合には、このファイルに設定パラメータのデフォルト値が書き込まれます。

– ユーザ毎の設定ファイルがない。

– または、ユーザ毎の設定ファイルに関連するパラメータが指定されていない。

最初に取得された値が各々のオプションに適用されます。

> **i** 「*ssh*」の設定とそのオペランドに関する詳細な情報は以下のサイトのOpenSSH のページから得ることができます。
>
> *http://www.openssh.org/manual.html*

次の手順に従います。

► 「*ssh*」を起動して、SSHv2 認証により iRMC S4 にログインします。

```
ssh -l [<user>] <iRMC_S4>
```

または

```
ssh [<user>@]<iRMC_S4>
```

<user>
: iRMC S4 へのログインに使用するユーザ名。<user> を指定しない場合は、*ssh* は、iRMC S4 にログインしようとしているローカルコンピュータ上のログインユーザ名をそのまま使用します。

<iRMC_S4>
: ユーザがログインしようとする iRMC S4 名または、iRMC S4 の IP アドレス。

例 : iRMC S4 への SSHv2 認証ログイン

次の *ssh* 呼び出しでは、65 ページ の「例 :「ssh -keygen」による RSA 鍵ペアの生成」で説明した通り「*ssh-keygen*」が公開 / 秘密 RSA 鍵のペアの生成に用いられたものと見なされます。また、公開鍵 *User1/.ssh/id_rsa.pub* は、iRMC S4 ユーザ「*user4*」のために iRMC S4 にロードされていると見なされます（67 ページを参照）。

ユーザは自身のローカルコンピュータから、「*$HOME/User1*」でログインユーザ「*user4*」を使用して、以下のように iRMC S4 "RX300_S82-iRMC" にログインすることができます。

```
ssh user4@RX300_S82-iRMC
```

4.3.3.4 例：公開 SSHv2 鍵

同じ公開 SSHv2 鍵を、RFC4716 フォーマットと OpenSSH フォーマットの双方で以下に示します。

RFC4716 フォーマットの公開 SSHv2 鍵

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20090401"
AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx
v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9Ar
JxjlhXUzlPPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGsfc+F
pGJ2iw==
---- END SSH2 PUBLIC KEY ----
```

OpenSSH フォーマットの公開 SSHv2 鍵

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx
v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9Ar
JxjlhXUzlPPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGwsfc+F
pGJ2iw== rsa-key-20090401
```

5 ビデオリダイレクション（AVR）

ビデオリダイレクション（AVR）機能を使用するには、有効な KVM ライセンスキーが必要です。

Java キャッシングを**無効にしないでください**。無効にすると AVR を起動できません。（デフォルトでは Java キャッシングは有効です）。

ビデオリダイレクション（AVR）では、リモートワークステーションから管理対象サーバのマウスとキーボードを制御したり、管理対象サーバから現在のグラフィックやテキストの出力を表示することができます。

AVR Java アプレットでは、バーチャルメディア機能を使用できます（109 ページ の「仮想メディアウィザード」の章を参照）。

本章では以下について説明します。

– AVR 設定の確認
– AVR の使用
– AVR ウィンドウのメニュー

5.1 要件：AVR 設定の確認

AVR を使用する前に、以下の重要な設定を確認してください。

管理対象サーバのグラフィックモードの設定

AVR は以下のグラフィックモードをサポートします。

解像度	リフレッシュレート [Hz]	Maximum 色深度 [bits]
640 x 480（VGA）	60; 75; 85	32
800 x 600（SVGA）	56; 60; 72; 75; 85	32
1024 x 768（XGA）	60; 70; 75; 85	32
1152 x 864	60; 70; 75	32
1280 x 1024（UXGA）	60; 70; 75; 85	16
1280 x 1024（UXGA）	60	24
1600 x 1200（UXGA）	60; 65	16
1680 x 1050	60	16
1920 x 1080	60	16
1920 x 1200	60	16

表 3: サポートされる画面設定

i VESA 準拠のグラフィックモードのみサポートされます。

サポートされるテキストモード

iRMC S4 は下記の共通テキストモードをサポートします。

- 40 x 25
- 80 x 25
- 80 x 43 ###
- 80 x 50

画面設定については、ご利用のオペレーティングシステムのヘルプシステムを参照してください。

キーボードの設定

リモートワークステーションのキーボードの言語設定が管理対象サーバと異なる場合、AVR のキーボードの言語設定を管理対象サーバと同じにする必要があります。

> **i** 以下の言語間のマッピングのみ可能です。
>
> - 英語
> - ドイツ語
> - 日本語
> - 英語
> - フランス語
> - スペイン語
>
> すべてのキーをマッピングできるわけではありません。機能しないキーがある場合は、ソフトキーボードを使用してください（84 ページを参照）。

5.2 AVR の使用

AVR の起動には次のオプションがあります。

► iRMC S4 Web インターフェースで「*ビデオリダイレクション（AVR）*」ページの「*ビデオリダイレクションの開始（Java Web Start）*」ボタンをクリックします（288 ページを参照）。

または、表示される場合は、

► iRMC S4 Web インターフェースのツリー構造で「*ビデオリダイレクション（JWS）*」リンクをクリックします。

「*ビデオリダイレクション*」ウィンドウ（AVR ウィンドウ）が開き、管理対象サーバの画面が表示されます。

5.2.1 AVR ウィンドウ

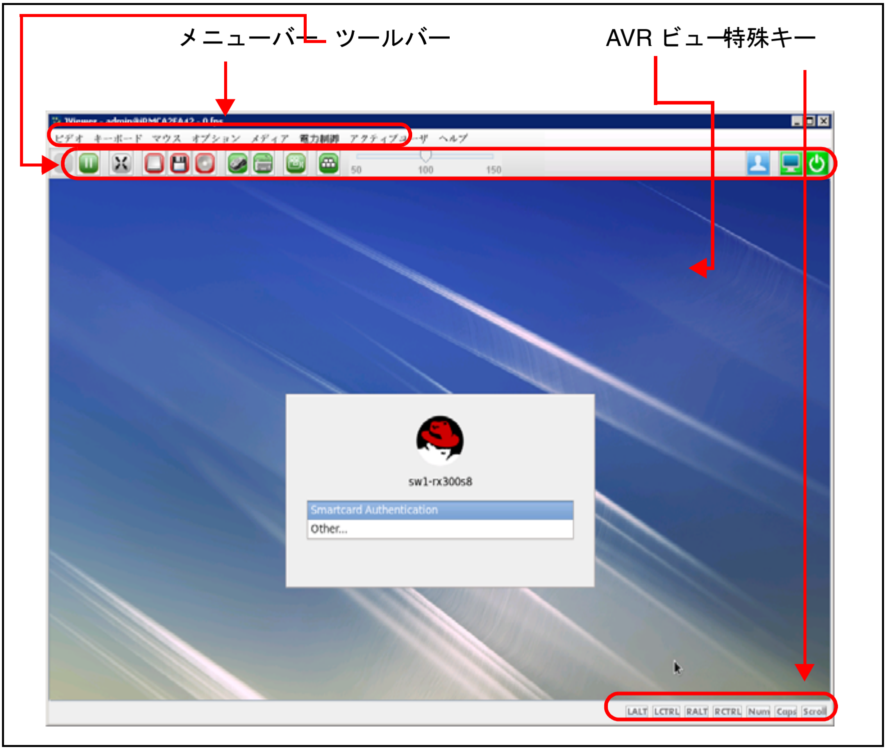


図 24: ビデオリダイレクション（AVR）画面

AVR ウィンドウには、以下のエレメントも含まれます。

- AVR メニューバーから、個々の AVR メニューにアクセスできます（86 ページを参照）。
- AVR ツールバーからさまざまな AVR ツールに直接アクセスして、AVR セッションの停止 / 開始、バーチャルメディア機能の使用、AVS セッションの記録、ホットキーの使用などができます（83 ページを参照）。
- ズームツールバーで AVR ビューを段階なく拡大 / 縮小できます（105 ページを参照）。
- AVR ウィンドウの右下にある統合された特殊キーで Windows のキーまたは特殊キーの組み合わせを使用できます。これらのキーは、ユーザ固有のキーボードで押しても送信されません（83 ページを参照）。

5.2.2 低帯域幅の使用

データ転送速度が低下した場合、現在の AVR セッションの色深度に対する帯域幅（bpp、ビット / ピクセル）を低く設定できます。

5.2.3 同時 AVR セッション

AVR は、同時に最大 2 つのユーザセッションで使用できます。1 つ目の開始された AVR セッションは、最初 *フルアクセス*モードで、サーバのフルコントロールができます。

前の AVR セッションがまだアクティブなときに 2 つ目の AVR セッションを開始

前の AVR セッション 1 がまだアクティブで *フルアクセス*モードのときに AVR セッション 2 を開始する場合、手順は次のようになります。

– セッション 1 の AVR ウィンドウで、「*仮想コンソールの特権を共有しています*」ダイアログが表示され、30 秒からカウントダウンします。

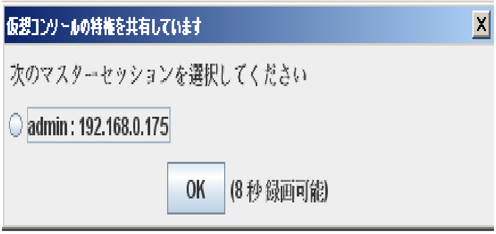


図 25: 「仮想コンソールの特権を共有しています」ダイアログボックスの「ユーザを許可」

仮想コンソールの許可

セッション 2 が *フルアクセス*モードに切り替わります。セッション 1 が *部分アクセス（ビデオのみ）*モードに切り替わります。

i セッション 1 のヴァーチャルメディア接続がクリアされます。

ビデオのみ許可

セッション 2 が*部分アクセス（ビデオのみ）*モードに切り替わります。このモードでは、サーバのキーボードおよびマウスの操作を表示するだけしかできません。*ビデオ*および*アクティブユーザ*機能を使用できます。

セッション 1 は*フルアクセス*モードのままになります。

アクセスを拒否

セッション 2 がアクセス拒否されて閉じます。セッション 1 は*フルアクセス*モードのままになります。

> **i** セッション 1 が「*OK*」で確定される前にカウンタの期限が切れると、セッション 2 が*フルアクセス*モードに切り替わります。セッション 1 が*部分アクセス（ビデオのみ）*モードに切り替わります。

「フルアクセス」セッションの終了

2 つの AVR セッションが現在アクティブのときに*フルアクセス*モードの一方の AVR セッションを終了すると、次のダイアログボックスが表示され、次のマスターセッション（つまり*フルアクセス*モードのセッション）を選択するように求められます。このダイアログボックスは、10 秒からカウントダウンします。

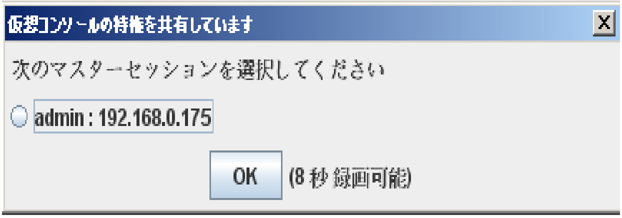


図 26: 「仮想コンソールの特権を共有しています」ダイアログボックスの「次のマスターセッションを選択してください」

このダイアログボックスではもう一方のセッションのユーザを選択でき、10 秒からカウントダウンします。

– このオプションを選択すると、もう一方のセッションが*フルアクセス*モードに切り替わります。

– このオプションの選択を解除すると、もう一方のセッションは*部分アクセス（ビデオのみ）*モードのままになります。

– 「*OK*」で確定される前にカウンタの期限が切れると、*部分アクセス（ビデオのみ）*モードのままになります。

5.2.4 「サーバ側モニタの表示オフ制御」機能

iRMC S4 の「*サーバ側モニタの表示オフ制御*」機能で、AVR セッション中期間中に管理対象サーバのサーバ側モニタの電源をオフにできます。この場合、AVR を使用するサーバのサーバ側モニタ上で行う入力と実行する操作は表示できません。識別灯が点滅して、サーバが「サーバ側モニタ OFF」モードであることを示します。

iRMC S4 Web インターフェースの「*ビデオリダイレクション*」ページの「*サーバ側モニタの表示オフ制御*」機能を設定します（288 ページを参照）。「*ビデオリダイレクション*」ページで、新しい AVR セッションが開始されると、サーバ側モニタが必ず自動的にオフに切り替わるように設定することもできます。

システムを適切に設定した後に、ツールバーの右から 2 番目のアイコンをクリックして AVR の「*Video*」メニューを使用しても、サーバのサーバ側モニタのオンとオフをリモートワークステーションから切り替えることができます。

「*サーバ側モニタの表示オフ制御*」オプション（292 ページを参照）が無効な場合、サーバ側モニタは必ずオンに切り替わり、切り替えることはできません。

サーバ側モニタの現在のステータスは AVR の「*Video*」メニューに示され、AVR ツールバーの右から 2 番目のアイコンを使用して表示されます（105 ページ の「AVR ツールバー」の項を参照）。

	サーバ側モニタがロックされている（オフに切り替えられている）ことを示します。つまり、AVR コンソールで行われる操作は、管理対象サーバのモニタには表示できません。このボタンをクリックすると、管理対象サーバのモニタのロックが解除され、アイコンが緑色に変わります。
	管理対象サーバのモニタがロック解除されている（オンに切り替えられている）ことを示します。つまり、AVR コンソールで行われる操作は、管理対象サーバのモニタに表示できます。このボタンをクリックすると、管理対象サーバのモニタがロックされ、アイコンが赤色に変わります。 「*サーバ側モニタの表示オフ制御*」オプション（292 ページを参照）が無効な場合、モニタのステータスを切り替えることはできません。

5.2.5 キーボードリダイレクション

キーボードリダイレクションは、AVR ウィンドウにフォーカスされている場合のみ機能します。

- ► キーボードリダイレクションが機能していないと思われる場合は、AVR ウィンドウをクリックしてみます。
- ► キーボードが反応しない場合は、AVR ウィンドウがビューモードになっていないかを確認します。フルコントロールモードに切り替える方法については、89 ページを参照してください。

特殊キーの組合せ

AVR は、通常のキーの組合せをすべてサーバに渡します。Windows キーなどの特殊キーは送信されません。[Alt] + [F4] などの一部の特殊キーの組合せは、クライアントのオペレーティングシステムに中断されるため、送信できません。このような場合は、統合された特殊キー、またはユーザ定義のホットキーや仮想キーボードのホットキーを使用してください。

統合された特殊キー

AVR ウィンドウの右下に、特殊キーのバーがあります。これらのキーは「スティックキー」として機能します。つまり、クリックすると押したままの状態（赤い文字で示されます）が続き、もう一度クリックするとまた元の位置に戻ります。

統合された特殊キーを使用すると、たとえば、ユーザ固有のキーボード上で押しても AVR に送信されない特殊キーの組合せを使用することができます。

図 27: AVR ウィンドウ - 統合された特殊キー

[LALT]
: Left Alt（ernate）キー（キーボードの [Alt] キーに相当）。

[LCTRL]
: Left CTRL キー（キーボードの左 [Ctrl] キーに相当）。

[RAlt]
: Right Alt（ernate）キー / Alt（ernate）Graphic キー（キーボードの [Alt Gr] キーに相当）。

RCTRL
: Right CTRL キー（キーボードの右 Ctrl キーに相当）。

Num
: Num キー。キーボードの右側にある数値キーをアクティブ / 非アクティブにします（キーボードの Num キーに相当）。

Caps
: Caps Lock キー（キーボードの Caps Lock キーに相当）。

Scroll
: Scroll キー。キーボードの Scroll キーに相当。

ソフトキーボード（仮想キーボード）

ソフトキーボード（仮想キーボードともいいます。図 28 を参照）には、キーボードの機能が表示されます。ソフトキーボードを使用するとすべてのキーの組合せを使用できます。つまり、ソフトキーボードでは実際のキーボードを完全に代替する機能が使用可能です。

ソフトキーボードは、AVR ウィンドウの「*キーボード*」メニューからアクティブにできます（87 ページ）。

図 28: ソフトキーボード（キーボードレイアウト：日本語（JP））

セキュアキーボード

iRMC S4 Web インターフェースを HTTPS 接続している場合、キーボード入力とマウスクリックを、リアルタイムで暗号化してから管理対象サーバに転送されるように設定できます（98 ページ の「AVR ウィンドウ - 「オプション」メニュー」の項を参照）。

5.2.6 マウスリダイレクション

管理対象サーバのマウスポインタは、リモートワークステーションのマウスと同期させて移動することができます。マウスリダイレクションの設定は、AVR ウィンドウの「*マウス*」の「*マウスモード*」で設定します（105 ページを参照）。

i マウスポインタの同期の設定は、管理対象サーバを実行するオペレーティングシステムでのみサポートされます。

マウスをコントロールするソフトウェアがアクティブな場合、マウスポインタを同期できないことがあります。

5.3 AVR ウィンドウのメニューとツールバー

AVR ウィンドウのメニューバーには以下のメニューがあります。

– 「*ビデオ*」メニューでは、AVR の設定と AVR のコントロールができます（87 ページを参照）。

– 「*キーボード*」メニューでは、*ソフトキーボード*を有効にして、キーボードの言語を選択できます。さらに、「*キーボード*」メニューでは、キーボードリダイレクション時に特殊キーを処理できます（91 ページを参照）。

– 「*マウス e* 」メニューでは、マウスの設定を行うことができます（96 ページを参照）。

– 「*オプション*」メニューでは、キーボードの暗号化の有効化 / 無効化、必要に応じてウィンドウサイズのリサイズ、AVR ウィンドウのメニューとダイアログボックスを表示する言語の設定（ドイツ語 / 英語 / 日本語）ができます（98 ページを参照）。

– 「*メディア*」メニューでは、*バーチャルメディア*機能を使用できます（100 ページを参照）。

– 「*電力制御* 」メニューでは、管理対象サーバの電源をオン / オフにしたり、次の起動時のサーバの動作を設定することができます（103 ページを参照）。

– 「*アクティブユーザ*」メニューには、現在アクティブな AVR セッションが表示されます（103 ページを参照）。

– 「*ヘルプ*」メニューでは、現在実行中の KVM リモートコンソール ユーティリティ のバージョン情報と、管理対象サーバの情報を表示できます（103 ページを参照）。

AVR ツールバーのアイコンを使用して、よく使用する AVR 機能に直接アクセスできます。

5.3.1 「ビデオ」メニュー

「*ビデオ*」メニューでは、AVR の設定と AVR のコントロールができます。

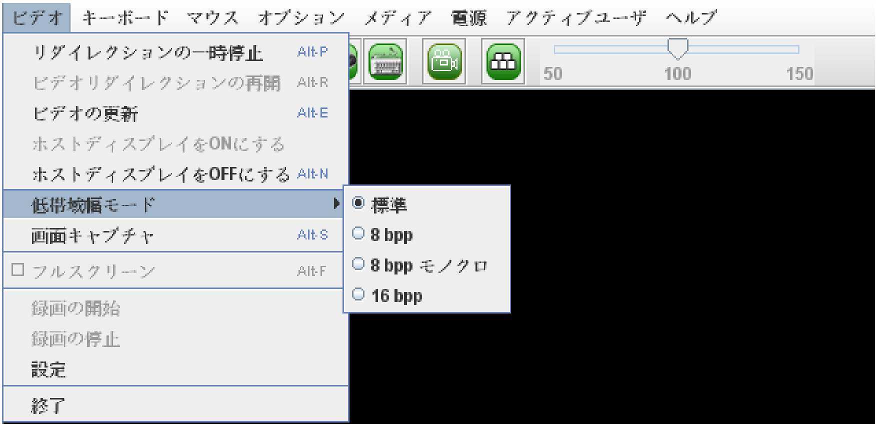


図 29: AVR ウィンドウ - 「ビデオ」メニュー

「*ビデオ*」メニューから以下の機能を選択できます。

リダイレクションの一時停止

AVR を一時停止し、AVR ビューを静止します。AVR ビューは AVR が再開されるまで静止したままになります。

ビデオリダイレクションの再開

AVR を再開し、AVR ビューを更新します。

ビデオの更新

AVR ビューを更新します。

ホストディスプレイを ON にする

このオプションが選択 / 選択解除されているかによって、管理対象サーバのサーバ側モニタをオンにします。

> **i** 次の場合、この機能はサーバ側モニタがオフの場合でも無効です。
>
> – ビューモードの場合。
>
> – 高解像度のグラフィックモードが管理対象サーバで設定されている（76 ページ の表 3 を参照）。
> サーバ側モニタの < ステータス > 表示： *Local Monitor always off*

ホストディスプレイを ＯＦＦ にする

このオプションが選択 / 選択解除されているかによって、管理対象サーバのサーバ側モニタをオフにします。

> **i** ビューモードの場合、この機能はサーバ側モニタがオフの場合でも無効です。

低帯域幅モード

データ転送速度が低下した場合、同じ iRMC S4 でのすべての AVR セッションの色深度に対する帯域幅（bpp、ビット / ピクセル）を低く設定できます。

「標準」

デフォルト。
これより低い帯域幅はありません。

8 bpp

8 bpp 色深度（256 色）。

8 bpp モノクロ

8 bpp 白黒深度（256 グレー階調）。

16 bpp

16 bpp 色深度（65536 色）。

画面キャプチャ

AVR ビューのスクリーンショットを作成し、関連する *CapturedScreen.jpeg* ファイルをネットワークステーションまたはネットワーク共有のディレクトリに格納できるブラウザを開きます。

フルスクリーン

フルスクリーンモードを有効 / 無効にします。

> **i** このオプションは、リモートワークステーションの画面解像度が管理対象サーバの画面解像度と同じ場合のみ有効にできます。

録画の開始

管理対象サーバのモニタに表示されるイベントのビデオ録画を作成します。

このボタンは、次の場合は無効です。

– 「*設定*」オプションでまだビデオ設定が行われていない（下記参照）。

– ビデオ録画が現在実行中。

録画の停止

ビデオ録画を停止します。このオプションは、ビデオ録画セッションが現在実行中の場合のみ有効にできます。

設定

「*ビデオ録画*」ダイアログボックスが開き、ビデオ録画に必要な設定を行うことができます。

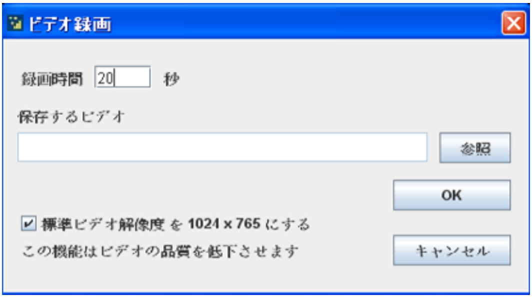


図 30: ビデオ録画の設定

録画時間

ビデオの継続期間（秒）。

参照

ブラウザダイアログが開き、ビデオを格納するコンピュータまたはネットワーク共有のディレクトリに移動できます。

保存するビデオ

「*参照*」で選択したディレクトリを表示します。

標準ビデオ解像度を 1024x768 にする

この場合、管理対象サーバのモニターでの解像度の変更ごとに個別のビデオファイルが作成されます。

このオプションが有効な場合、管理対象サーバのモニタの実際のビデオ解像度に関係なく、1024x768 という正規化されたビデオ解像度がビデオ出力全体に適用されます。これにより、ビデオの品質が低下することがあります。

OK

設定をアクティブにして、ダイアログボックスを閉じます。「*録画の開始*」ボタンが有効になります。

キャンセル

設定をアクティブにして、ダイアログボックスを閉じます。

終了

ユーザ固有の AVR セッションを終了します。

5.3.2 AVR ウィンドウ - 「キーボード」メニュー

「*キーボード*」メニューでは、キーボードリダイレクション時に特殊キーを処理できます（83 ページ の「キーボードリダイレクション」の項を参照）。

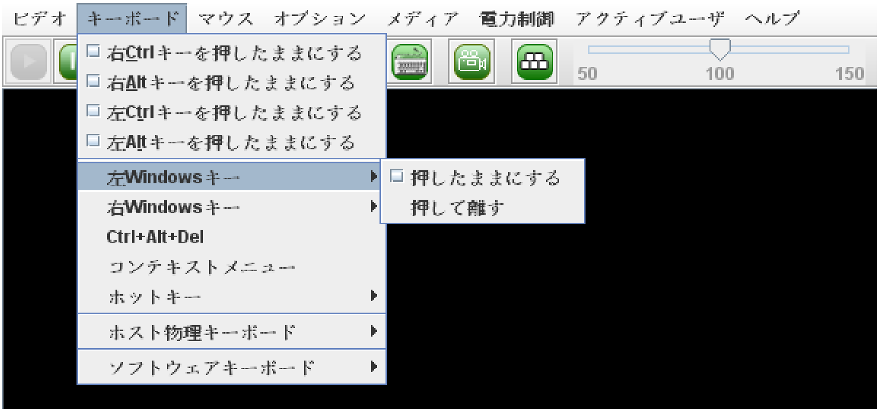


図 31: AVR Window - 「キーボード」メニュー

「*キーボード*」メニューから以下の機能を選択できます。

右 Ctrl キーを押したままにする
　右の [Ctrl] キーを押したままの状態にします。

右 Alt キーを押したままにする
　右の [Alt] キーを押したままの状態にします。

左 Ctrl キーを押したままにする
　左の [Ctrl] キーを押したままの状態にします。

左 Alt キーを押したままにする
　左の [Alt] キーを押したままの状態にします。

左 Windows キー
　「*押したままにする*」が有効な場合に左の Windows キーを押したままの状態にします。有効でない場合は、「*押して離す*」が適用されます。

右 Windows キー
　「*押したままにする*」が有効な場合に右の Windows キーを押したままの状態にします。有効でない場合は、「*押して離す*」が適用されます。

Ctrl+Alt+Del
　[Ctrl]+[Alt]+[Del] のキーの組み合わせを適用します。

コンテキストメニュー

管理対象サーバで実行中のアプリケーションまたはオペレーティングシステムの適切なコンテキストメニューを開きます。

ホットキー

ユーザ固有のホットキーの定義と適用ができます。

すでに定義されているホットキーを適用するには、次の手順に従います。

1. 「*ホットキー*」をクリックします。

   i ホットキーを定義する場合、AVR ツールバーの*ホットキー*アイコンも使用できます（105 ページ の「AVR ツールバー」の項を参照）。

2. 「*ホットキーの追加*」アイテムの下に、すでに定義されているホットキーのリストが表示されるので、必要なホットキーをクリックします。

新しいホットキーを定義するには、次の手順に従います。

1. 「*ホットキー*」–「*ホットキーの追加*」をクリックします。

   「*ユーザー定義マクロ*」ダイアログボックスが開き、すでに定義されているユーザ定義マクロが表示されます（ここでは A、B）:

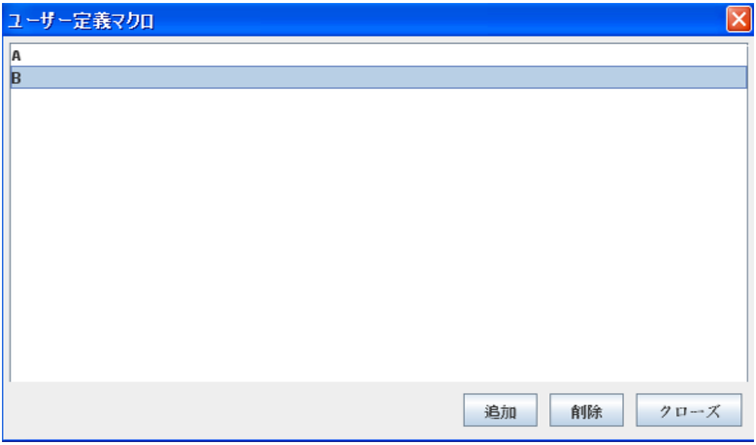


図 32: AVR ウィンドウ - 「キーボード」メニュー - 「ホットキーの追加」–「ユーザー定義マクロ」(1)

2. 「*追加*」をクリックして新しいユーザ定義マクロを定義します。

   「*マクロの追加*」ダイアログボックスが開きます。

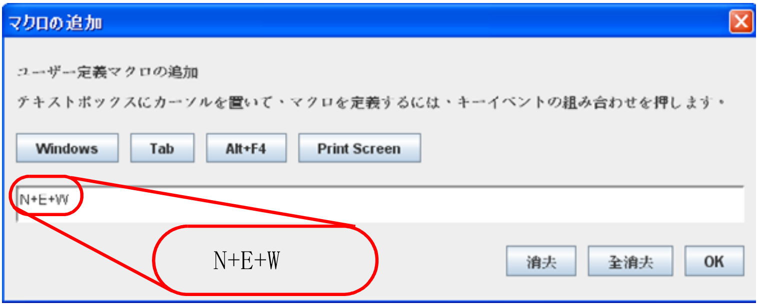


図 33: AVR ウィンドウ - 「キーボード」メニュー - 「ホットキーの追加」- 「マクロの追加」

3. キーボードの「*Windows*」、「*Tab*」、「*Alt+F4*」、「*Print Screen*」ボタンおよびキーを使用して、最大 6 個の任意のキーの組み合わせを入力します。

   入力した組み合わせは「*マクロの追加*」ダイアログボックスに表示されます。「*全消去*」または「*消去*」をクリックすると、すべてのキーまたは画面の一番右のキーを削除できます。

4. 「*OK*」をクリックして新しいホットキーをアクティブにします。

   新しいホットキーが「*ユーザー定義マクロ*」ダイアログボックスに表示されます。

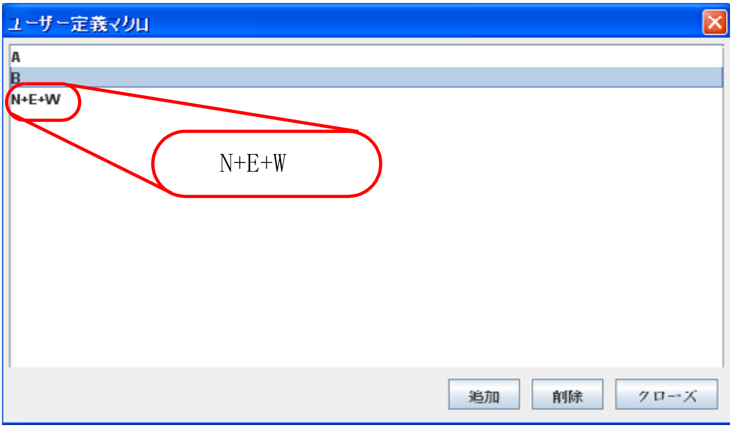


図 34: AVR ウィンドウ - 「「キーボード」メニュー - 「ホットキーの追加」- 「ユーザー定義マクロ」(2)

5. ホットキーを削除するには、対応するエントリ（94 ページ の図 34 に表示される例の「B」）を選択して「*削除*」をクリックします。

6. 「*クローズ*」をクリックして「*ユーザー定義マクロ*」ダイアログボックスを閉じます。

ホスト物理キーボード

管理対象サーバのキーボードで使用する言語。以下のオプションを選択できます。

– 「*自動検出*」（デフォルト値）
– *English (United States)*
– *French*
– *German (Germany)*
– *日本語*
– *Spanish*

「*自動検出*」を選択した場合、AVR は、キーボードの言語が管理対象サーバおよびリモートワークステーションと同じと見なします。

ソフトウェアキーボード

ソフトキーボード（仮想キーボード）を表示します。

目的の言語でソフトキーボードを表示するには、次の手順に従います。

1. マウスポインタを「*ソフトウェアキーボード*」アイテムに移動します。

   選択可能なソフトキーボード言語のリストが表示されます。

2. 目的の言語をリストから選択します。

   選択した言語のソフトキーボードが表示されます。

図 35: AVR ウィンドウ - 「キーボード」メニュー - 「ソフトウェアキーボード」

5.3.3 AVR ウィンドウ - 「マウス」メニュー

「マウス」メニューでは、マウスリダイレクションの設定を行うことができます。

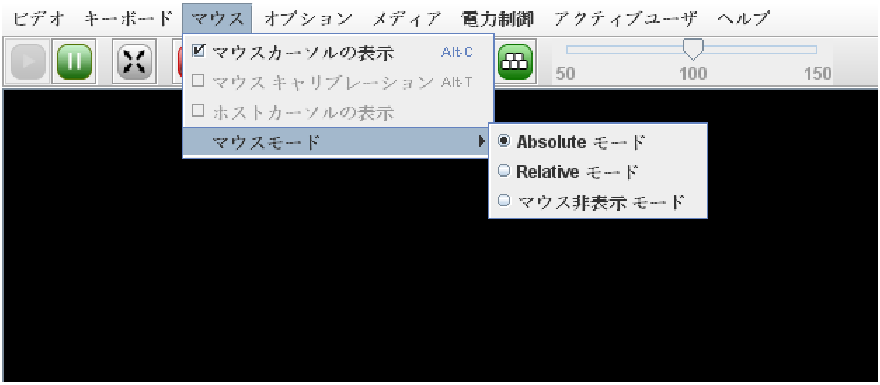


図 36: AVR ウィンドウ - 「マウス」メニュー

「マウス」メニューから次の機能を選択できます。

カーソルの表示
: AVR の使用時に、リモートワークステーションのマウスポインタを表示 / 非表示にします。

マウス キャリブレーション
: 相対マウスモードを調整する場合に使用します。このオプションは、「*M マウスモードe*」-「*Relative モード*」が選択されている場合のみ有効です。

> **i** 相対マウスモードでは、管理対象サーバのマウスポインタが、減速してリモートワークステーションのマウスポインタに従います。

ホストカーソルの表示

管理対象サーバのマウスポインタに加えて、追加のマウスポインタを表示します。

> **i** マウスポインタのハードウェアアクセレレーションを最大値に設定し、Matrox G200e を搭載する場合、iRMC S4 のマウスポインタがアクティブになります。このモードでは、マウスポインタは通常 1 つしか表示されません。この場合「*ホストカーソルの表示*」オプションを使用して、管理対象サーバを参照する 2 つ目のマウスポインタを表示できます。

マウスモード

マウスモード（「*Absolute モード*」、「*Relative モード*」、「*マウス非表示モード*」のいずれか）を指定します。「*マウス非表示 モード*」の場合、リモートワークステーションのマウスポインタは表示されません。

> **i** デフォルト設定 :「*Absolute mouse mode*」。
>
> 常に「*Absolute モード*」を使用してください。古いオペレーティングシステム（RedHat 4 など）の場合のみ、「*Absolute モード*」を使用できないことがあります。

> **i** LSI WEBBIOS の場合、「*マウス非表示 モード*」を使用してください。

5.3.4 AVR ウィンドウ - 「オプション」メニュー

「*オプション*」メニューでは、キーボード / マウスの暗号化の有効化 / 無効化、必要に応じてウィンドウサイズのリサイズ、AVR ウィンドウのメニューとダイアログボックスを表示する言語の設定ができます。

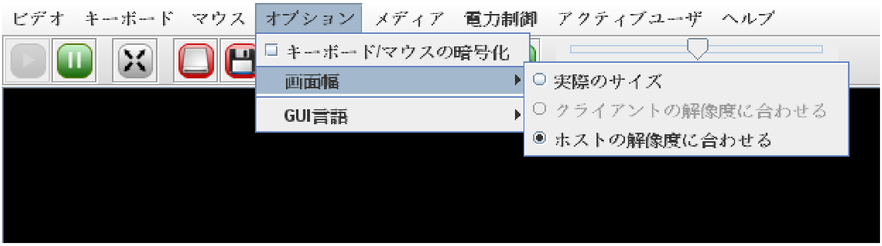


図 37: AVR ウィンドウ - 「オプション」メニュー

「*オプション*」メニューから以下の機能を選択できます。

キーボード / マウスの暗号化

キーボード / マウスの暗号化の有効化 / 無効化ができます。つまり、キーボード入力とマウスクリックは、リアルタイムで暗号化されてから管理対象サーバに転送されます。

i このオプションは、HTTPS 接続で iRMC S4 Web インターフェースに接続されている場合は選択できません。この場合、iRMC S4 Web インターフェースと管理対象サーバ間のすべての通信は SSL 暗号化されます。

画面幅

AVR ウィンドウのサイズを、実際のサイズで表示するか、管理対象サーバのサーバ側モニタの解像度に合わせるか、リモートワークステーションのモニターの解像度に合わせるかを指定します。

実際のサイズ

AVR ウィンドウは全画面サイズに拡張されます。

クライアントの解像度に合わせる

このオプションは、リモートワークステーションの画面解像度が管理対象サーバの画面解像度以下の場合のみ有効にできます。

i リモートワークステーションおよび管理対象サーバの画面解像度が同じ場合、AVR ツールバーの「*フルスクリーン*」アイコンが有効になります（105 ページ の「AVR ツールバー」の項を参照）。

ホストの解像度に合わせる

リモートワークステーションの画面解像像が管理対象サーバの画面解像より高い場合、AVR ウィンドウ

は自動的に調整されます。

これは通常の作業環境です。

GUI 言語

AVR ウィンドウのメニューとダイアログボックスを表示する言語（「*DE - Deutsch*」、「*EN - English*」、「*JA - 日本語*」）を指定します。

この選択は、AVR セッションを起動する iRMC S4 Web インターフェースに設定された GUI 言語を使用して事前に設定されています。

5.3.5 AVR ウィンドウ - 「メディア」メニュー

「メディア」から仮想メディアウィザードを起動できます。仮想メディアウィザードでは、リモートワークステーションにバーチャルメディアデバイスとしてメディアを接続したり接続解除したりできます（109 ページ の「仮想メディアウィザード」の章を参照）。

図 38: AVR ウィンドウ - 「メディア」メニュー

仮想メディアウィザード...

「*仮想メディアウィザード...*」をクリックして*仮想メディアウィザード*を起動して、リモートワークステーションにヴァーチャルメディアデバイスとしてメディアを接続したり接続解除したりできます（109 ページ の「仮想メディアウィザード」の章を参照）。

5.3.6 AVR ウィンドウ - 「電力制御」メニュー

「*電源制御*」メニューを使用して、サーバの電源投入 / 切断やリブートを行うことができます。さらに、次の起動時のサーバの動作を設定することができます。

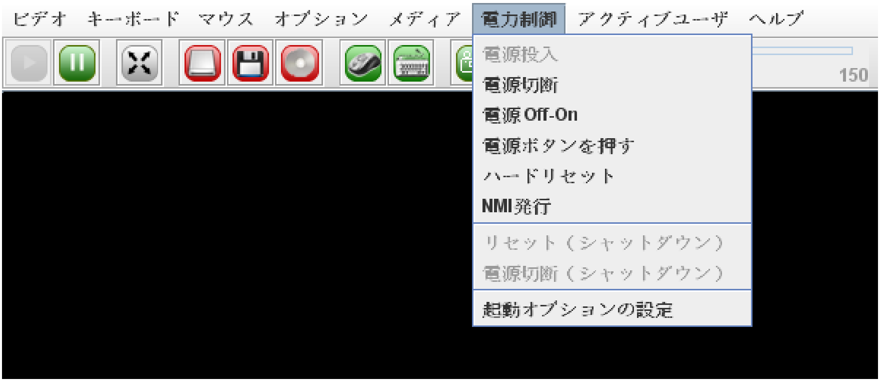


図 39: AVR ウィンドウ - 「電力制御」メニュー

電源投入
サーバの電源を投入します。

電源切断
オペレーティングシステムの状態にかかわらず、サーバの電源を切断します。

電源 Off-On
サーバの電源が完全に切断され、設定した時間の経過後、再び投入されます。この時間は、「*ASR&R オプション*」グループの「*パワーサイクル間隔*」フィールドで設定できます（225 ページを参照）。

電源ボタンを押す
インストールされているオペレーティングシステムと設定されている動作に依存して、電源オフボタンを短く押してさまざまな動作をトリガできます。これらの動作では、コンピュータのシャットダウンや、スタンバイモードへの切り替えができます。

ハードリセット
オペレーティングシステムの状態にかかわらず、サーバを完全に再起動します（コールドスタート）。

NMI 発行

マスク不可能な割り込み（NMI：Non-Maskable Interrupt）を初期化します。NMI は、システムの標準の割り込みマスクテクノロジで無視できるプロセッサ割り込みです。

リセット（シャットダウン）

正常にシャットダウンして、再起動します。
このオプションは、ServerView エージェントがインストールされていて、かつ、iRMC S4 にサインオンして「接続中」の場合のみ使用できます。

電源切断（シャットダウン）

グレースフルシャットダウンし、電源を切断します。
このオプションは、ServerView エージェントがインストールされていて、かつ、iRMC S4 にサインオンして「接続中」の場合のみ使用できます。

起動オプションの設定

このアイテムをクリックすると「*起動オプションの設定*」ダイアログが開き、**次の**起動時のシステムの動作を設定できます。

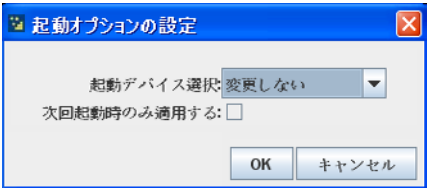


図 40: 「電力制御」メニュー - 「起動オプションの設定」

起動デバイス選択

起動するストレージメディア。以下のオプションを選択できます。

– 「*変更しない*」前と同じストレージメディアからシステムを起動します。
– 「*PXE/iSCSI*」: システムをネットワーク上の PXE あるいは iSCSI から起動します。
– 「*Hard Drive*」: システムをハードディスクから起動します。
– 「*CD/DVD-ROM*」: システムを CD/DVD から起動します。
– 「*Floppy*」: システムをフロッピーディスクから起動します。

– 「*Bios セットアップ*」: 起動時にシステムが BIOS セットアップに入ります。

次回起動時のみ適用する
行われた設定は、次の起動時にのみ適用されます。

5.3.7 AVR ウィンドウ - 「アクティブユーザ」メニュー

「*アクティブユーザ*」メニューには、現在 AVR を使用しているユーザが表示されます。緑色のビュレットはユーザ固有のセッションであることを示します。

図 41: AVR ウィンドウ - 「アクティブユーザ」メニュー

5.3.8 AVR ウィンドウ - 「ヘルプ」メニュー

JViewer の一般情報を表示するほかに、「*ヘルプ*」メニューの「*サーバ情報*」ダイアログボックスには、iRMC S4 Web インターフェースの「*システムの概要*」ページの「*システム情報*」に定義された情報が表示されます（132 ページ の「システムの概要 - サーバの一般情報」の項を参照）。

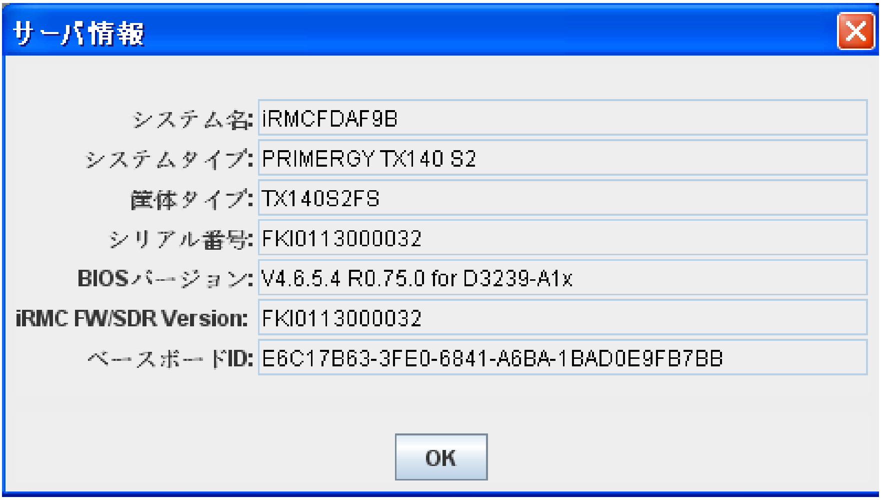


図 42: AVR ウィンドウ - 「ヘルプ」メニュー

5.3.9 AVR ツールバー

AVR ツールバーのアイコンを使用して、よく使用する AVR 機能に直接アクセスできます。マウスポインタをアイコンの上に移動すると、ツールチップ形式のヒントが表示されることがあります。

> **i** 「*部分アクセス（ビデオのみ）*」モードでは、「*Video*」および「*アクティブユーザ*」アイコンを使用できます。

図 43: AVR ウィンドウ - 「プリファレンス」メニュー

サーバ側でビデオリダイレクションが「*Num Lock On*」モードで実行された場合、クライアント側も「*Num Lock ON*」に切り替わります。

次のリストに「*ServerList* 」ウィンドウのアイコンとその意味を示します。

	AVR を再開し、AVR ビューを更新します。
	AVR を一時停止し、AVR ビューを静止します。AVR ビューは AVR が再開されるまで静止したままになります。
	フルスクリーンモードを有効 / 無効にします。
	ハードディスク /USB リダイレクションがこの AVR セッションに確立されているか（緑色）されていないか（赤色）を示します。アイコンをクリックすると*仮想メディアウィザード*が起動します（109 ページ の「仮想メディアウィザード」の章を参照）。
	フロッピーリダイレクションがこの AVR セッションに確立されているか（緑色）されていないか（赤色）を示します。アイコンをクリックすると*仮想メディアウィザード*が起動します（109 ページ の「仮想メディアウィザード」の章を参照）。
	CD/DVD リダイレクションがこの AVR セッションに確立されているか（緑色）されていないか（赤色）を示します。アイコンをクリックすると*仮想メディアウィザード*が起動します（109 ページ の「仮想メディアウィザード」の章を参照）。

表 4: 「ServerList」ウィンドウのアイコン

	リモートワークステーションのマウスポインタが AVR ウィンドウで表示可能か（緑色）または不可能か（グレー表示）を示します。アイコンをクリックすると、2 つのモードを切り替えることができます。
	ソフトキーボードを表示します（詳細については 91 ページ の「AVR ウィンドウ - 「キーボード」メニュー」の項を参照）。
	ビデオ設定がすでに設定されているかどうかによって、ビデオ録画を開始するか、ビデオ設定を行う「*ビデオ録画*」ダイアログが開きます（詳細については 87 ページ の「「ビデオ」メニュー」の項を参照）。
	使用可能なホットキーのリストが表示されます。ホットキーを適用するには、関連するアイテムをクリックします。ホットキーの定義の詳細については、91 ページ の「AVR ウィンドウ - 「キーボード」メニュー」の項を参照してください。
	ズームツールバーで AVR ビューを段階なく拡大 / 縮小できます。
	現在アクティブな各 AVR セッションについて、AVR セッションを開始した iRMC S4 ユーザと、AVR セッションを開始したリモートワークステーションの IP アドレスを表示します。
 	iRMC S4 Web インターフェースの「*サーバ側モニタの表示オフ制御*」が有効な場合、このトグルボタンで次の状態を切り替えることができます。 管理対象サーバのモニタのロックが解除されていることを示します。つまり、AVR コンソールで行われる操作は、管理対象サーバのモニタに表示できます。このボタンをクリックすると、管理対象サーバのモニタがロックされます。 管理対象サーバのモニタがロックされていることを示します。つまり、AVR コンソールで行われる操作は、管理対象サーバのモニタに表示できません。このボタンをクリックすると、管理対象サーバのモニタのロックが解除されます。

表 4: 「ServerList」ウィンドウのアイコン

	このトグルボタンで、管理対象サーバの電源のオン / オフを切り替えることができます。
	管理対象サーバの電源が現在オンであることを示します。このボタンをクリックすると、管理対象サーバの電源をオフにすることを確定するダイアログが表示されます（即時電源切断）。
	管理対象サーバの電源が現在オフであることを示します。このボタンをクリックすると、管理対象サーバの電源をオンにすることを確定するダイアログが表示されます。

表 4: 「ServerList」ウィンドウのアイコン

6 仮想メディアウィザード

Virtual Media ウィザードを使用するには、有効なバーチャルメディア（VM）のライセンスキーが必要です。

Virtual Media ウィザードを使用すると、リモートワークステーションにソースを設定している「仮想」ドライブを、管理対象サーバで使用できるようになります。管理対象サーバとリモートワークステーション間のヴァーチャルメディア接続は、AVR Java アプレットを使用して確立されます。「*Virtual Media Options*」ページで行った設定に基づいて、合計最大 12 個のバーチャルメディアを接続し、次のタイプを選択できます。

– 物理フロッピーまたはフロッピーイメージ（最大 4 個）
– 物理 CD/DVD または CD/DVD ISO イメージ（合計最大 4 個）
– ハードディスクドライブまたはハードディスク /USB イメージ（合計最大 4 個）

リモートメディアを物理的にリモートワークステーションに配置する必要はありません。このリモートワークステーションからアクセス可能な任意のネットワーク共有に配置することもできます。

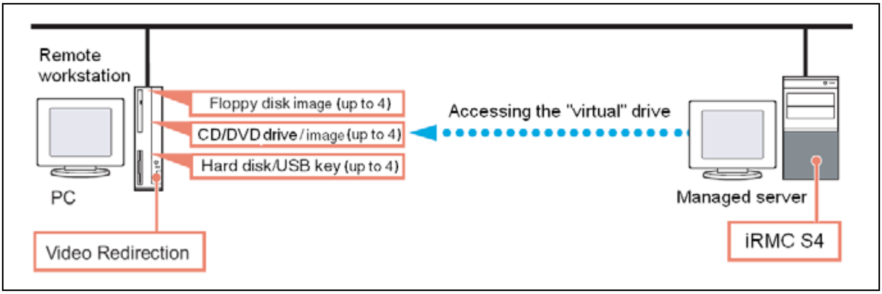


図 44: リモート接続で提供されるバーチャルメディア

6.1 リモートワークステーションへのバーチャルメディアの提供

仮想ドライブのソースをリモートワークステーションに提供する場合、仮想機能は次のデバイスタイプをサポートします。

– フロッピー
– CD ISO イメージ
– DVD ISO イメージ
– CD、DVD

i 光学ストレージメディア（CD、DVD）は自動的に表示されます（選択用に表示されます）。

i バーチャルメディアとして接続されたデバイスは、iRMC S4 によって、USB 接続されたデバイスとして認識されます。USB 接続がない場合（USB ドライバがない場合）は、これらは使用できません。

仮想ドライブを使用して、リモートワークステーションから PRIMERGY にオペレーティングシステムをインストールすることができます（361 ページ の「iRMC S4 によるオペレーティングシステムのリモートインストール」の章を参照）。

この節では以下について説明します。

- Virtual Media ウィザードの起動
- 「*Virtual Media*」ダイアログボックスでのバーチャルメディアの処理
  – バーチャルメディアセッションへのストレージメディアの提供
  – バーチャルメディアとしてのストレージメディアの接続
  – バーチャルメディア接続のクリア

6.1.1 Virtual Media ウィザードの起動

AVR Java アプレットを使用して Virtual Media ウィザードを起動します（288 ページ の「ビデオリダイレクション（AVR）- ビデオリダイレクション（AVR）の開始」の項を参照）。

▶ iRMC S4 Web インターフェースを起動します（120 ページ の「iRMC S4 Web インターフェースへのログイン」の項を参照）。

▶ 「*Advanced Video Redirection*」ページを開き、「*ビデオリダイレクションの開始（Java Web-Start）*」をクリックしてビデオリダイレクションを開始します（288 ページ の「ビデオリダイレクション（AVR）- ビデオリダイレクション（AVR）の開始」の項を参照）。

その結果、AVR ウィンドウが開かれます。

▶ AVR ウィンドウのメニューバーで次を選択します。
「*Media*」–「*Virtual Media Wizard...*」

または、ツールバーの 3 つのバーチャルメディアアイコンのいずれかをクリックします。

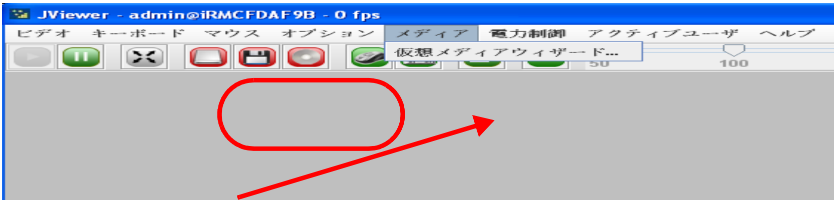


図 45: AVR ウィンドウ - 「Media」- 「Virtual Media Wizard...」

「*Virtual Media*」ダイアログボックスが開きます。

6.1.2 「Virtual Media」ダイアログボックス

iRMC S4 Web インターフェースの「*Virtual Media*」ページで行った設定に基づいて、「*Virtual Media*」ダイアログボックスに、次の 3 つのメディアタイプのそれぞれのパネルが 0 ～ 4 つ表示されます。

- フロッピーキーメディア（フロッピーイメージ）
- CD/DVD メディア ISO イメージ
  - CD/DVD メディア ISO イメージ
  - CD/DVD ドライブ（物理 CD/DVD）
- ハードディスク /USB キーメディア
  - ハードディスク /USB キーイメージ
  - 物理ドライブ（固定ドライブ）

i 物理ストレージドライブは、Linux システムにマウントする必要があります。

図 46: 「Virtual Media」ダイアログボックス

「*Status*」パネルには、ヴァーチャルメディア接続で現在使用可能なストレージメディアと、仮想ストレージメディアとして現在接続されているストレージメディアの両方に関する情報が表示されます。

6.1.3 バーチャルメディアへのストレージメディアの提供

i AVR セッション中はいつでも、以下のオプションを実行できます。

– 追加のバーチャルメディア接続を既存のバーチャルメディア接続に追加します。

– 個々のバーチャルメディア接続の接続を解除します。

目的のタイプのストレージメディア（DVD イメージなど）を提供するには、以下の手順に従います。

i 物理ドライブが自動的に表示されます。イメージを提供する場合のみ参照する必要があります。

► 「*Vitual Media*」ダイアログボックスの適切なパネルで「*Browse*」をクリックします。

「*Open*」ファイルブラウザダイアログボックスが開きます。

► 「*Open*」ダイアログボックスで、リモートステーションからバーチャルメディアとして使用できるようにするストレージメディアのディレクトリに移動します。

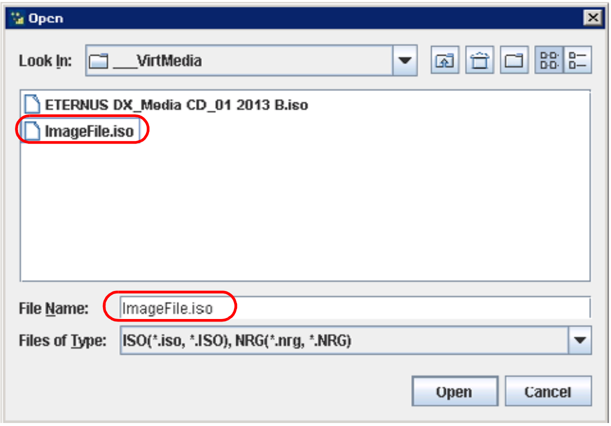


図 47: 「Open」ダイアログボックス（Windows）

► 「*Files of Type*」で必要なデバイスタイプを選択します。

i 物理ストレージドライブは、Linux システムにマウントする必要があります。

- ►「*File Name*」でバーチャルメディアとして接続するストレージメディアを指定します。
  - – ISO イメージ（ISO/NRG イメージ）の場合はファイル名を入力します。または、エクスプローラでファイル名をクリックします。
  - – ドライブの場合はドライブ名を入力します。次に例を示します。
    - – D ドライブの場合は「D」（Windows）
    - – */dev/...*（Linux）
- ►「*Open* 」をクリックして選択を確定します。

  選択したストレージメディアがバーチャルメディアとして使用可能になり、「*Virtual Media*」ダイアログボックスの対応するパネルに表示されます。

「Storage Devices」ダイアログの表示 (Windows)

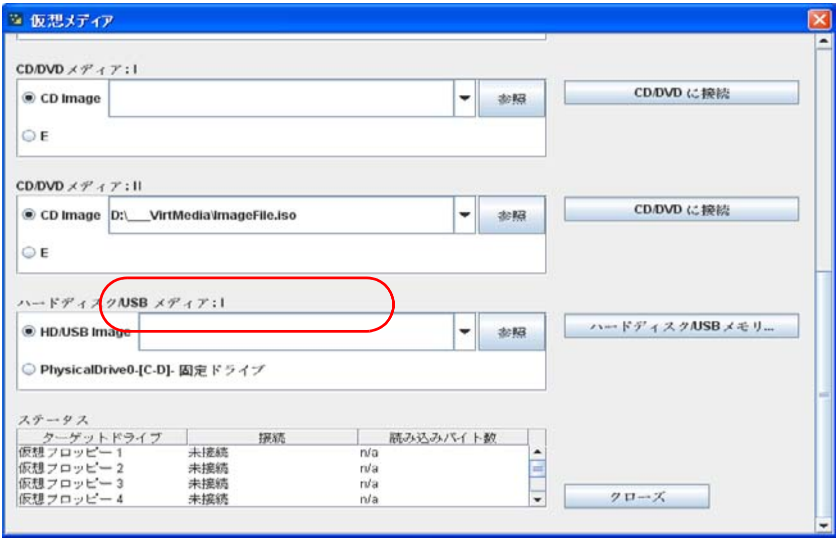


図 48: 「Virtual Media」ダイアログボックス：提供したストレージメディアが表示されます。

- ► 対応する「*Connect...*」ボタンをクリックして提供したストレージメディアをバーチャルメディアとして接続します。

選択したストレージメディアがバーチャルメディアとして使用可能になり、「*Virtual Media*」ダイアログボックスの対応するパネルに表示されます。

「Storage Devices」ダイアログの表示 (Windows)

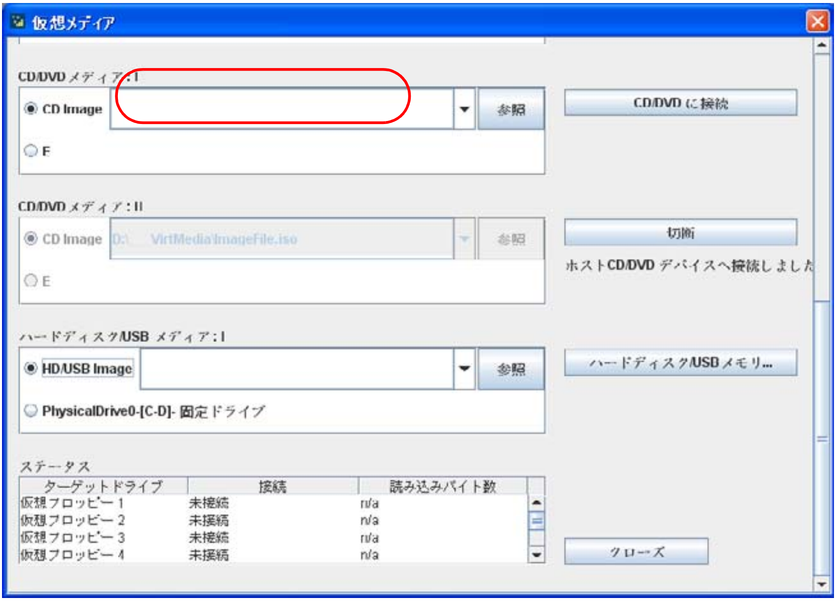


図 49: 「Virtual Media」ダイアログボックス：提供したストレージメディアが表示されます。

6.1.4 バーチャルメディア接続のクリア

i 仮想接続は、次の場合に自動的に解放されます。

- AVR セッションの接続が解除される。
- 2 番目の AVR セッションの「フルアクセス」リクエストが成功したことにより、バーチャルメディア接続を確立した AVR セッションが「読み取り専用」モードに変わる。
- 「*Virtual Media Options*」ページで行った設定が変更される（297 ページを参照）。

▶ 「*Virtual Media*」ダイアログを開きます（111 ページ の「Virtual Media ウィザードの起動」の項を参照）。

▶ ストレージデバイスの 「安全な取り外し」を行います。つまり、ストレージデバイスにアクセスしているアプリケーションやプログラムがないことを確認してから取り外します。

▶ *バーチャルメディア*接続をクリアするには、対応する「*Disconnect*」ボタンをクリックします。

7 iRMC S4 Web インターフェース

iRMC S4 は固有のオペレーティングシステムを持つだけでなく、Web サーバとしても稼動し、固有のインターフェースを提供します。iRMC S4 Web インターフェースのメニューとダイアログ ボックスの表示言語は、ドイツ語、英語、日本語のいずれかを選択できます。

iRMC S4 Web インターフェースで値を入力するときに、ツールチップ形式のヒントが表示されることがあります。

i 以下に説明するソフトウェアは Independent JPEG Group の成果に一部基づいています。

7.1 iRMC S4 Web インターフェースへのログイン

► リモートワークステーションから Web ブラウザを開いて、iRMC S4 の DNS 名（構成されている場合）（240 ページを参照）または IP アドレスを入力します。

iRMC S4 にディレクトリサービスへの LDAP アクセスが構成されているかどうかによって、表示されるログイン画面が異なります「*LDAP 有効*」オプションについて、263 ページを参照）。

> **i** ログイン画面が表示されない場合は、LAN 接続（43 ページ の「LAN インターフェースのテスト」の項を参照）を確認してください。

– iRMC S4 にディレクトリサービスへの LDAP アクセスが構成されておらず「*LDAP 有効*」オプションが無効）、かつ「*常に SSL ログインを使用する*」オプション（263 ページを参照）が無効な場合、次のログイン画面が表示されます。

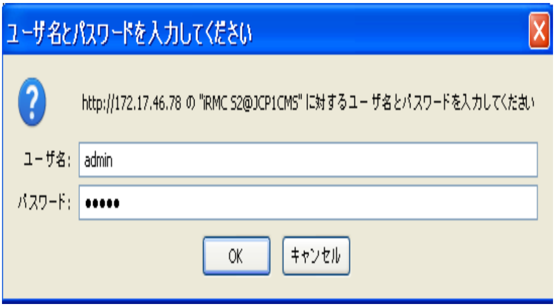


図 50: iRMC S4 Web インターフェースのログイン画面（LDAP アクセスが構成されておらず、かつ、「常に SSL ログインを使用する」オプションが無効な場合）

► デフォルトの管理者アカウントのデータを入力してください。

ユーザ名 : admin

パスワード : admin

> **i** *ユーザ名とパスワード*は、大文字小文字を区別します。

セキュリティ上の理由から、一度ログインした後は、新しい管理者アカウントを作成してデフォルトの管理者アカウントを削除するか、少なくともパスワードを変更するようにお勧めします（255 ページ の「「ユーザ “<name>” 構成」- ユーザ設定（詳細）」 を参照）。

▶ 「*OK*」をクリックして、入力を確定してください。

– iRMC S4 にディレクトリサービスへの LDAP アクセスが構成されている
「*LDAP 有効*オプションが有効」または *常に SSL ログインを使用する*オプションが有効」：

図 51: iRMC S4 Web インターフェースのログイン画面（LDAP アクセスが構成されている場合）

i ユーザ名とパスワードは、送信時に必ず SSL により保護されます。「*安全（SSL）*」オプションが有効な場合、Web ブラウザと、iRMC S4 間のすべての通信は、HTTPS によって行われます。

▶ デフォルトの管理者アカウントのデータを入力してください。

ユーザ名 : admin

パスワード : admin

i セキュリティ上の理由から、一度ログインした後は、新しい管理者アカウントを作成してデフォルトの管理者アカウントを削除するか、少なくともパスワードを変更するようにお勧めします（255 ページ の「「ユーザ “<name>” 構成」- ユーザ設定（詳細）」 を参照）。

► 「*ログイン*」をクリックして、ログインを確定します。

iRMC S4 Web インターフェースが開き、*「システム情報」*ページ（131 ページを参照）が表示されます。

7.2 必要なユーザ権限

表 5 に、iRMC S4 Web インターフェースの各々のファンクションを使用するために必要な権限の概要を示します。

iRMC S4 Web インターフェースのファンクション	IPMI レベルで許可				必要な iRMC S4 固有の権限			
	OEM	Administrator	Operator	ユーザ	ユーザアカウント変更権限	iRMC S4 設定変更権限	AVR 使用権限	リモートストレージ使用権限
「*システムの概要*」ページの表示	X	X	X	X				
識別灯のオン / オフ	X	X	X	X				
「*資産タグ設定*」の設定						X		
*オペレーティングシステムの情報の*編集 1)						X		
「*System Components* 」ページの表示	X	X	X	X				
「*Reset Memory Error Counter*」						X		
「*SPD データを表示*」	X	X	X	X				
「*Network Inventory* 」ページの表示	X	X	X	X				
「*RAID Controller*」ページの表示	X	X						
「*Physical Discs* 」ページの表示	X	X						
RAID 物理ディスクの識別（「*Locate* 」ボタン）	X	X				X		
「*資産タグ設定*」の設定						X		
「*Physical Drives* 」ページの表示	X	X						
RAID 物理ディスクの識別（「*Locate* 」ボタン）	X	X				X		
「*BIOS パラメータ設定のバックアップ/ リストア*」ページの表示。2)	X	X	X	X				
「*BIOS パラメータ設定のバックアップ/ リストア*」*の編集。設定*2)	X	X						
「BIOS アップデート設定」ページの表示。2)	X	X	X	X				
BIOS アップデートの実行 2)	X	X						

表 5: 固有の iRMC S4 Web インターフェースを使用するための権限

iRMC S4 Web インターフェースのファンクション	IPMI レベルで許可				必要な iRMC S4 固有の権限			
	OEM	Administrator	Operator	ユーザ	ユーザアカウント変更権限	iRMC S4 設定変更権限	AVR 使用権限	リモートストレージ使用権限
「*iRMC S4 情報*」ページの表示	X	X	X	X				
「*Reboot iRMC S4*」	X	X						
iRMC S4 へのライセンスキーのアップロード						X		
「*その他のオプション*」の設定						X		
「*Save iRMC S4 Time* 」ページの表示	X	X	X	X				
「iRMC S4 Time Options」の変更						X		
「*iRMC S4 ファームウェア設定の保存*」ページの表示					X	X		
「*ユーザ設定*」の選択					X			
他のすべての設定の選択						X		
iRMC S4 の設定を WinSCU XML 形式でインポート					X	X		
「*認証データアップロード*」ページの表示 / 編集						X		
「*自己署名証明書の作成。*」ページの表示と編集						X		
「*iRMC S4 ファームウェアアップデート*」ページの表示	X	X	X	X				
ファームウェアセレクタの設定	X	X						
「*ファイルからのファームウェアアップデート*」の実行						X		
TFTP 経由でのファームウェアアップデート「*iRMC S4 TFTP 設定*」。						X		
「*Power On/Off*」ページの表示。	X	X	X	X				
「*起動オプション*」の変更。						X		
「*電源制御*」の使用	X	X	X					
「*電源制御オプション*」ページの表示と編集						X		

表 5: 固有の iRMC S4 Web インターフェースを使用するための権限

iRMC S4 Web インターフェースのファンクション	IPMI レベルで許可				必要な iRMC S4 固有の権限			
	OEM	Administrator	Operator	ユーザ	ユーザアカウント変更権限	iRMC S4 設定変更権限	AVR 使用権限	リモートストレージ使用権限
「*電源装置情報*」ページの表示	X	X	X	X				
「*消費電力制御*」ページの表示と編集						X		
*現在の全体消費電力*ページの表示 2)						X		
消費電力モニタリング履歴 ページの表示と編集 2)。						X		
「*ファン*」ページの表示	X	X	X	X				
ファンテストの開始 （「*ファンテスト*」グループ）	X	X	X	X				
「*ファンテスト時刻*」の設定（「*ファンテスト*」グループ）						X		
個々のファンの選択（「*システムファン*」グループ）						X		
「*異常時動作 / シャットダウン待ち時間*」の設定						X		
「*温度*」ページの表示	X	X	X	X				
温度センサの異常時動作の指定						X		
「*電圧*」ページの表示。	X	X	X	X				
「*電源ユニット*」ページの表示。	X	X	X	X				
冗長電源の設定						X		
「*センサの状態*」ページの表示。	X	X	X	X				
「*システムイベントログ内容*」ページの表示。	X	X	X	X				
システムイベントログ（SEL）のクリア	X	X	X					
「*ログの保存*」（SEL）。	X	X	X	X				
SEL エントリ表示の重要度の定義	X	X	X	X				
「*iRMC S4 イベントログ内容*」ページの表示。	X	X						
内部イベントログ（iEL）のクリア	X	X						
「*ログの保存*」（iEL）	X	X						

表 5: 固有の iRMC S4 Web インターフェースを使用するための権限

iRMC S4 Web インターフェースのファンクション	IPMI レベルで許可				必要な iRMC S4 固有の権限			
	OEM	Administrator	Operator	ユーザ	ユーザアカウント変更権限	iRMC S4 設定変更権限	AVR 使用権限	リモートストレージ使用権限
SEL エントリ表示の重要度の定義	X	X						
「*システムイベントログ設定*」ページの表示。	X	X	X	X				
「Default Web Interface display filtering」の変更						X		
SEL モードの変更						X		
ヘルプデスク情報の変更						X		
「*サーバ管理情報*」の表示と編集。						X		
「*ネットワークインターフェース*」ページの表示と編集。						X		
「*ポート番号およびネットワーク*」表示と編集。 「サービス」ページの表示と編集。						X		
「*DNS 構成*」ページの表示と編集。						X		
「*SNMP トラップ送信設定*」ページの表示と編集。						X		
「*Email 設定*」ページの表示と編集。						X		
「*iRMC S4 ユーザ情報*」ページの表示と編集。					X			
「*ディレクトリ サービス構成*」ページの表示と編集 。						X		
「*CAS 設定*」ページの表示					X	X		
「*CAS 一般設定*」の編集						X		
「*CAS ユーザ権限と許可*」の編集					X			
「*BIOS テキストコンソール*」ページの表示	X	X	X	X				
「*BIOS コンソールリダイレクションオプション*」の変更。						X		
「*ビデオリダイレクション(AVR)*」ページの表示と編集。							X	
「*Virtual Media*」ページの表示と編集								X

表 5: 固有の iRMC S4 Web インターフェースを使用するための権限

iRMC S4 Web インターフェースのファンクション	IPMI レベルで許可				必要な iRMC S4 固有の権限			
	OEM	Administrator	Operator	ユーザ	ユーザアカウント変更権限	iRMC S4 設定変更権限	AVR 使用権限	リモートストレージ使用権限
「*Remote Image Mount*」ページの表示と編集								X
「*Media Options*」ページの表示と編集								X
「*iRMC S4 SSH アクセス*」の開始。	X	X	X	X				
SSH ログイン	X	X	X	X				
「*iRMC S4 Telnet Access*」の起動	X	X	X	X				
Telnet ログイン	X	X	X	X				

1) 実行中のエージェントがない場合のみの動作

2) システムによっては使用できない機能

表 5: 固有の iRMC S4 Web インターフェースを使用するための権限

7.3 ユーザインターフェースの構造

iRMC S4 Web インターフェースの構造を以下に示します。

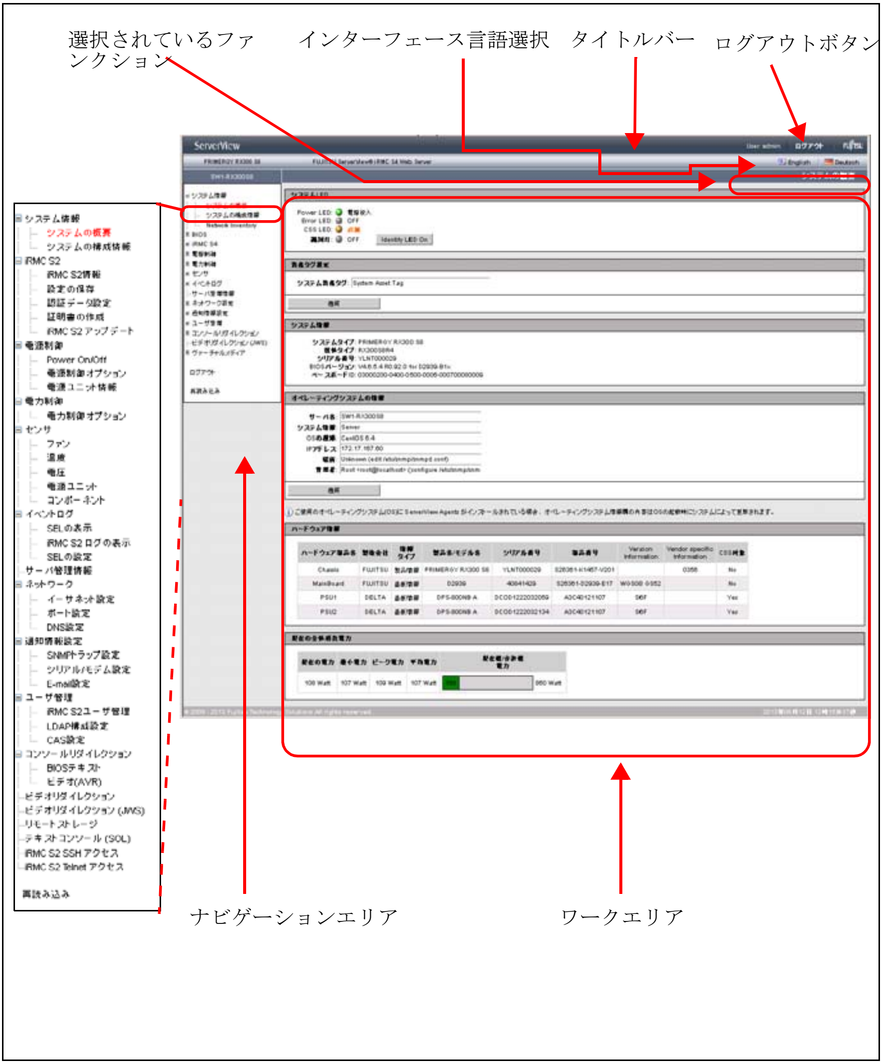


図 52: iRMC S4 Web インターフェースの構造

iRMC S4 Web インターフェースの言語の選択

ワークエリアの上の黒いバーの右に、旗のアイコンがあります。このアイコンをクリックして、iRMC S4 Web インターフェースのナビゲーションエリア、メニューおよびダイアログボックスを表示する言語（ドイツ語、英語、日本語のいずれか）を選択してください。

ナビゲーションエリア

ナビゲーションエリアには、iRMC S4 の個々のファンクションをタスクベースに並べたメニューツリー構造があります。これらのリンクのいずれかをクリックすると（図 52 :「*システムの概要*」）、そのリンクが有効になり、そのファンクションのワークエリアが表示され、任意の出力、ダイアログボックス、オプション、リンクおよびボタンが表示されます。

個々の iRMC S4 ファンクションの下に、「*ログアウト*」と「*再読み込み*」のリンクがあります。

- 「*ログアウト*」は、ダイアログボックスでの確認の後、iRMC S4 のセッションを終了させることができます。iRMC S4 にディレクトリサービスへの LDAP アクセスが構成されているかどうかによって、セッション終了後に表示されるログイン画面が異なります（「*LDAP 有効*」オプションについて、263 ページを参照）。

  – iRMC S4 にディレクトリサービスへの LDAP アクセスが構成されておらず（「*LDAP 有効*」オプションが無効）、かつ「*常に SSL ログインを使用する*」オプション（263 ページを参照）が無効な場合、次のログイン画面が表示されます。

図 53: ログインページ（ログアウト後）

「*ログイン*」ボタンをクリックして iRMC S4 Web インターフェースのログイン画面を表示します（120 ページ の図 50 を参照）。必要な場合、再びログインできます。

– iRMC S4 にディレクトリサービスへの LDAP アクセスが構成されている場合
（「*LDAP 有効*」*オプションが有効*）、かつ「*常に SSL ログインを使用する*」オプション（263 ページを参照）が無効な場合、適切なログイン画面が表示されます（121 ページ の図 51 を参照）。

- 「*再読み込み*」ボタンをクリックすると、iRMC S4 Web インターフェースの内容を再読み込みすることができます。

i 再読み込みの代わりに、内容が定期的に自動更新されるようにインターフェースを設定することもできます（238 ページ の「自動リフレッシュ有効」を参照）。

7.4 システム情報 - 管理対象サーバの情報

「*システム情報*」エントリには、以下のページへのリンクが含まれます。

– 132 ページ の「システムの概要 - サーバの一般情報」
– 137 ページ の「システム構成情報 - サーバ構成情報」
– 140 ページ の「Network Inventory」

7.4.1 システムの概要 - サーバの一般情報

「*システムの概要*」ページには、以下の情報が表示されます。

– システムの状態
– 資産タグ設定
– システム（一般情報）
– 管理対象サーバのオペレーティングシステム
– システムの FRU（フィールド交換可能ユニット）/IDPROM
– 管理対象サーバの現在の全体消費電力

また、「*システムの概要* 」ページでは、管理対象サーバにユーザ固有の資産タグを入力できます。

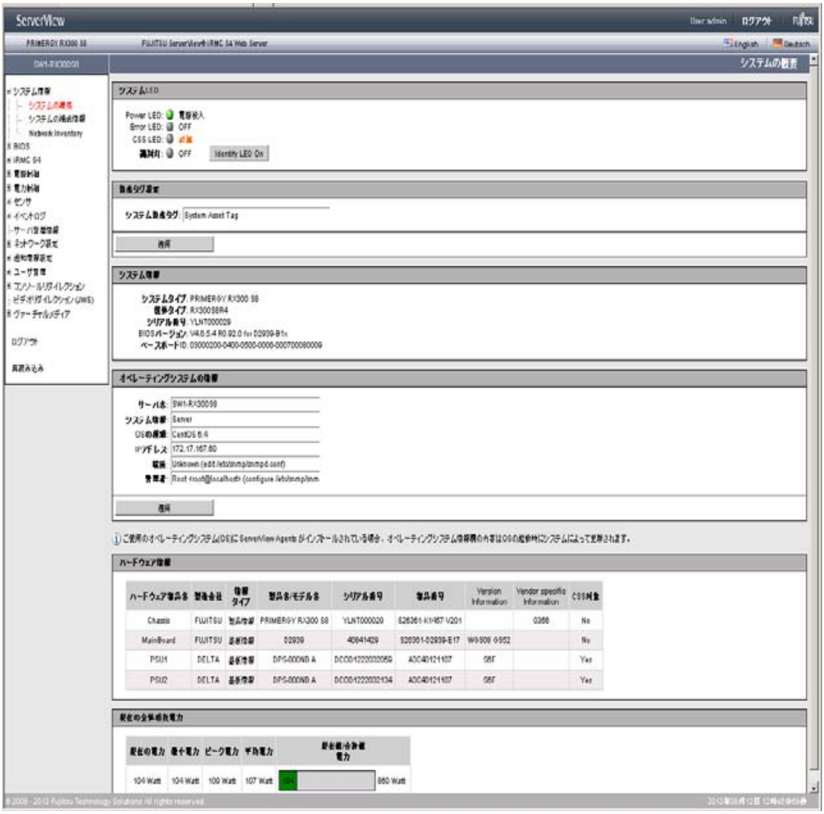


図 54: 「システムの概要」ページ

システム LED

保守ランプ、CSS LED、識別灯のステータスが、「*システム LED*」に表示されます。PRIMERGY の識別灯のオン / オフを切り替えることもできます。

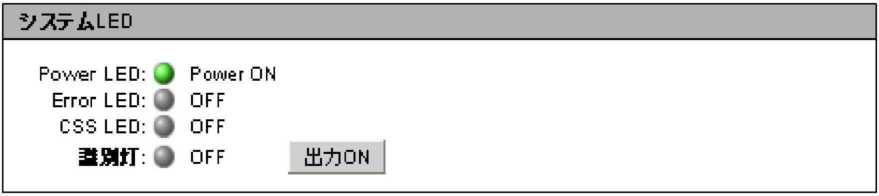


図 55: 「システムの概要」ページ - システム LED

Power LED

サーバの電源状態。
以下のステータスが可能です :

– 点灯 :「Power ON」（緑色）
– 消灯 :「Power OFF」（オレンジ色）

Error LED

サーバの保守ランプに関する情報 :

ステータス情報 (iRMC S4)	**サーバのグローバルエラー LED (サーバ)**	**システム全体の状態**
消灯	点灯しない	クリティカルイベントなし
点灯	赤く点灯	非 CSS コンポーネントに故障予兆イベントあり
点滅	赤く点滅	クリティカルイベントあり

CSS LED

サーバの CSS（Customer Self Service）に関する情報 :

ステータス情報 (iRMC S4)	**サーバの CSS LED サーバ**	**システム全体の状態**
消灯	点灯しない	サーバ稼働中
点灯	オレンジに点灯	CSS コンポーネントに故障予兆イベントあり
点滅	オレンジに点滅	CSS コンポーネント故障

識別灯

サーバ ID。
以下のステータスが可能です :

– On （青色）
– 消灯（灰色）

出力 ON/ 出力 OFF

「*出力 ON/ 出力 OFF*」ボタンで、PRIMERGY の識別灯の点灯 / 消灯を切り替えます。

資産タグ設定

「*資産タグ設定*」で、管理対象サーバにユーザ固有の資産タグを入力できます。

ユーザ固有の資産タグを使用して、インベントリ番号または選択したその他の ID をサーバに割り当てることができます。

Windows 対応システムの場合は、このユーザ固有の資産タグは WMI（Windows Management Instrumentation）より自動的に提供されます。資産タグは、社内ツールで評価したり、企業管理システム（CA Unicenter など）の統合に使用できます。

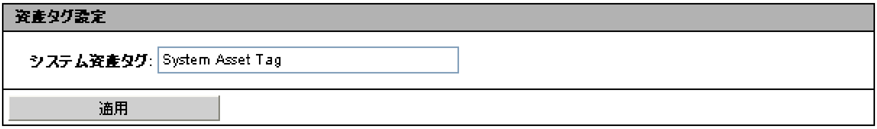


図 56: 「システムの概要」ページ - 資産タグ設定

システム資産タグ

ここに資産タグを入力できます。

► 「*適用*」をクリックして資産タグを適用します。

システム情報

「*システム情報*」には、管理対象サーバの情報が表示されます。

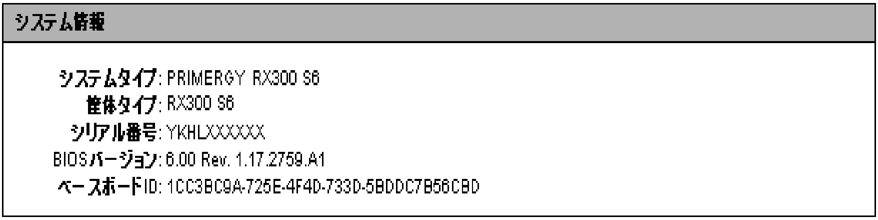


図 57: 「システムの概要」ページ - システム情報

オペレーティングシステムの情報

「*オペレーティングシステムの情報*」には、管理対象サーバのオペレーティングシステムに関する情報が表示されます。

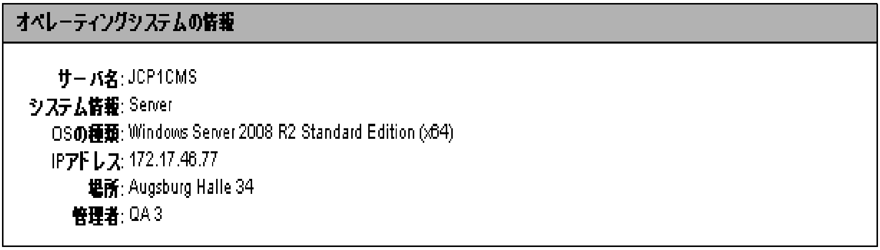


図 58: 「システムの概要」ページ - オペレーティングシステムの情報

i ServerView エージェントが実行中でない場合は、「*オペレーティングシステムの情報*」グループのすべてのフィールドを編集できますが、実行中は編集できません。

ServerView エージェントの起動後に、ユーザの初期値はエージェントが自動検出した値に上書きされます。

ハードウェア情報

FRU（**F**ield **R**eplaceable **U**nit）に関する情報が「*System FRU/IDPROM Information*」に表示されます。FRU はシステムから解放し取り外すことのできるコンポーネントです。「*CSS 対象*」列には、各コンポーネントの CSS（**C**ustomer **S**elf **S**ervice）機能のサポートの有無が示されます。

ハードウェア情報

ハードウェア部品名	製造会社	情報タイプ	製品名/モデル名	シリアル番号	部品番号	バージョン/その他	CSS対象
Chassis	FUJITSU	製品情報	PRIMERGY RX300 S8	YKHLXXXXXX	S26361-K1265-V1XX	0246	No
MainBoard	FUJITSU	基板情報	D2759	31122813	S26361-D2759-A12	WGS03 GS51	No
PSU STD	DELTA	基板情報	POWERSUPPLY 350W	E5495001010921Y000322	S26113-E549-V50-01	Rev 01	No

図 59: 「システムの概要」ページ - ハードウェア情報

現在の全体消費電力

i このオプションは、一部の PRIMERGY サーバではサポートされていません。

現在の全体消費電力

現在の電力	最小電力	ピーク電力	平均電力	現在値/合計値電力	
62 Watt	62 Watt	63 Watt	62 Watt	62	450 Watt

図 60: 「システムの概要」ページ - 現在の全体消費電力

「*現在の全体消費電力*」には、設定された間隔で測定されたサーバの消費電力量の現在値、最小値、最大値、平均値が表示されます。

グラフィカルな表示でも、サーバの可能な最大消費電力量と現在の消費電力量を比較して表示しています。

7.4.2 システム構成情報 - サーバ構成情報

「*システム構成情報*」ページには、CPU およびメインメモリモジュールに関する情報が表示されます。「*CSS 対象*」列には、各コンポーネントの CSS（**C**ustomer **S**elf **S**ervice）機能のサポートの有無が示されます。

以下のステータスアイコンは、システムコンポーネントの状態を示します。

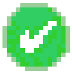
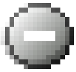
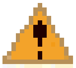
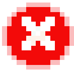
	OK：コンポーネントの状態は良好です。
	コンポーネントのスロットが空いています。
	警告：コンポーネントの状態が低下しています。
	欠陥：コンポーネントに欠陥があります。

表 6: システムコンポーネントの状態

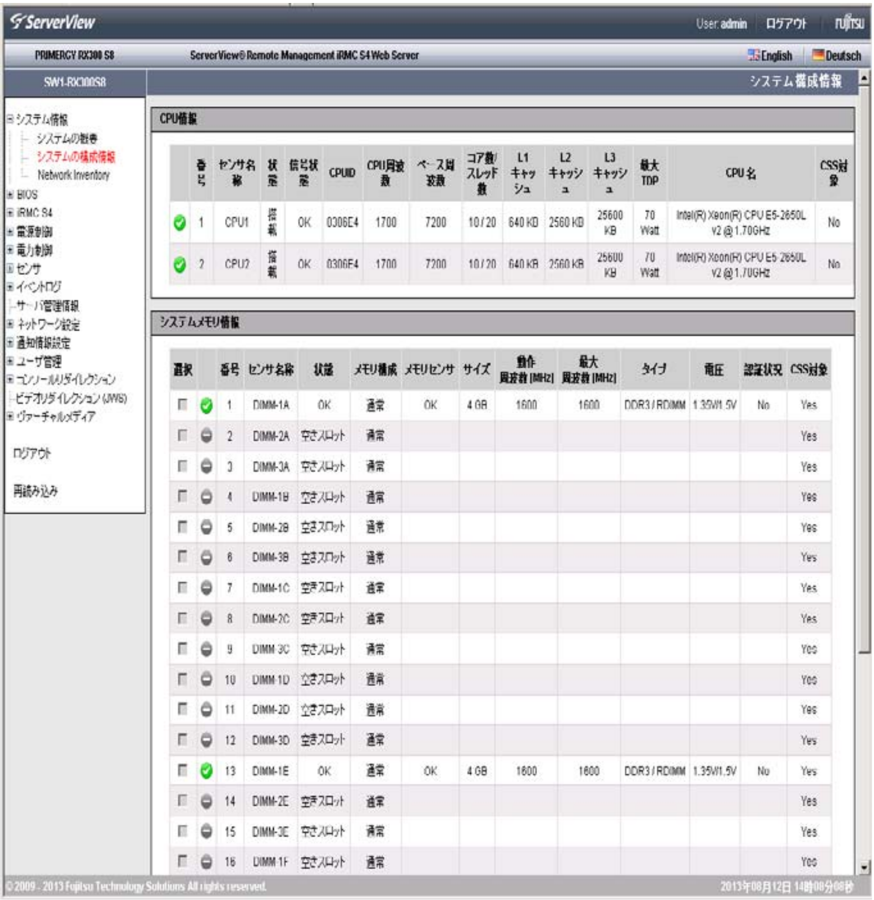


図 61: 「システム構成情報」ページ

> **i** TPM（Trusted Platform Module）をサポートする PRIMERGY サーバの場合、このページは TPM が有効か無効かを示します。

CPU 情報

このグループでは、管理対象の PRIMERGY サーバの CPU の状態、ID、CSS の機能、および性能に関する情報を提供します。

システムメモリ情報

このグループでは、管理対象の PRIMERGY サーバのメインメモリモジュールの状態、ID、CSS の機能、および性能に関する情報を提供します。

選択

個々のメモリモジュールを選択し、適用する動作を「*一覧からメモリアクションを選択してください*」から選択できます。

全てにチェック

すべてのメモリモジュールを選択します。

全て非選択

選択を解除します。

一覧からメモリアクションを選択してください

このリストから、選択したメモリに適用する動作を選択します。

> **i** iRMC S4 または ServerBlade の場合、エラーカウンタが 0 に設定された状態で新しいモジュールが自動的に検出されるため、エラーカウンタを明示的にリセットする必要はありません。

選択モジュールへの適用

選択した動作を選択したモジュールに適用します。

SPD データを表示 / すべて選択解除

「*View SPD Data / No SPD Data*」ボタンをクリックすると、個々のメモリコンポーネントのベンダー固有の詳細（SPD（**S**erial **P**resence **D**etect）データ）を表示 / 非表示できます。

メモリの SPD データは、コンポーネントおよびサーバに統合された EEPROM に保存されるので、BIOS によって自動的にメモリコンポーネント（RAM、DIMM）が検出されます。

7.4.3 Network Inventory

「*Network Inventory*」ページには、iRMC S4 の Ethernet ポートに関する情報が表示されます。

図 62: 「Network Inventory」ページ

7.5 「RAID 情報」- RAID システムに関する情報

「*RAID 情報*」エントリおよび関連するページは、以下の要件が満たされる場合のみ表示されます。

– アウトオブバンド対応 RAID コントローラを管理対象サーバで使用できる。

– サーバの電源が入っていない。

「*RAID 情報*」エントリには、次のページへのリンクが含まれます。

– 142 ページ の「「RAID コントローラ」- RAID コントローラおよび関連するバッテリーに関する情報」

– 144 ページ の「「物理ディスク」- RAID 物理ディスクに関する情報」

– 146 ページ の「「論理デバイス」- RAID 論理ドライブに関する情報」

7.5.1 「RAID コントローラ」- RAID コントローラおよび関連するバッテリーに関する情報

管理対象サーバの各 RAID コントローラについて、「*RAID コントローラ*」ページに RAID コントローラおよび関連するバッテリーのステータスに関数する情報が表示されます。

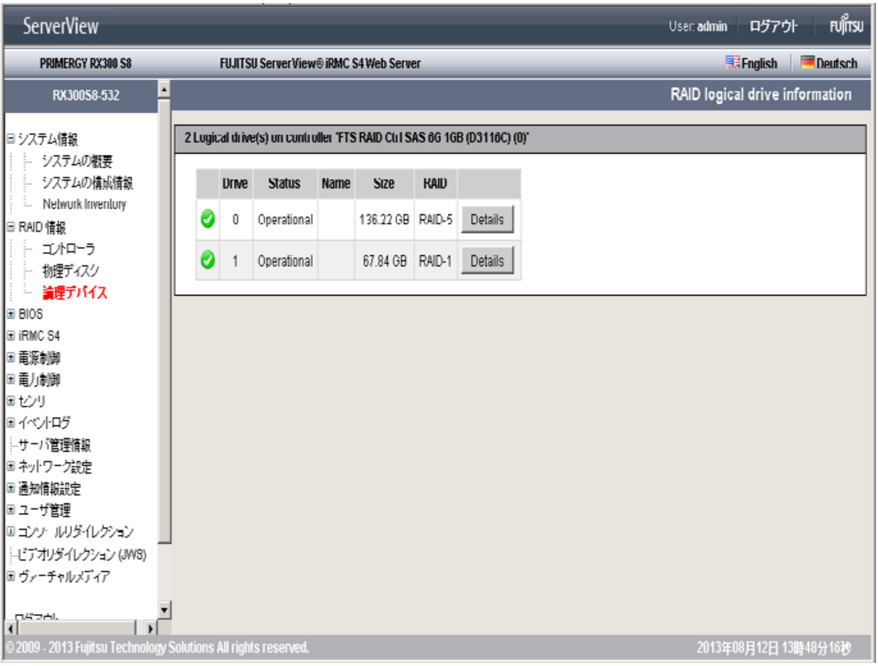


図 63: 「RAID 情報」- 「コントローラ」ページ

Details

「*Details*」をクリックすると、RAID コントローラ / バッテリーに関する詳細情報が表示されます。

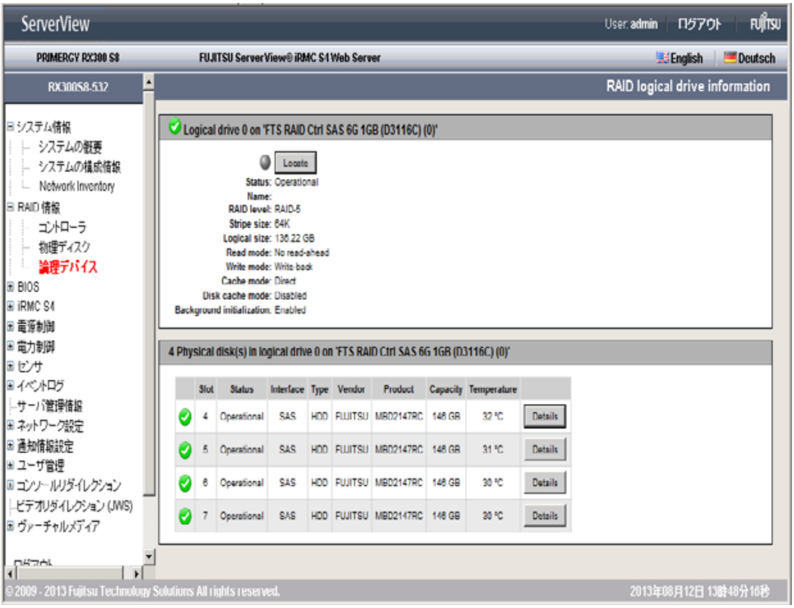


図 64: RAID コントローラの詳細

7.5.2 「物理ディスク」- RAID 物理ディスクに関する情報

「*物理ディスク*」ページには、管理対象サーバの各 RAID 物理ディスクに関する情報が表示されます。

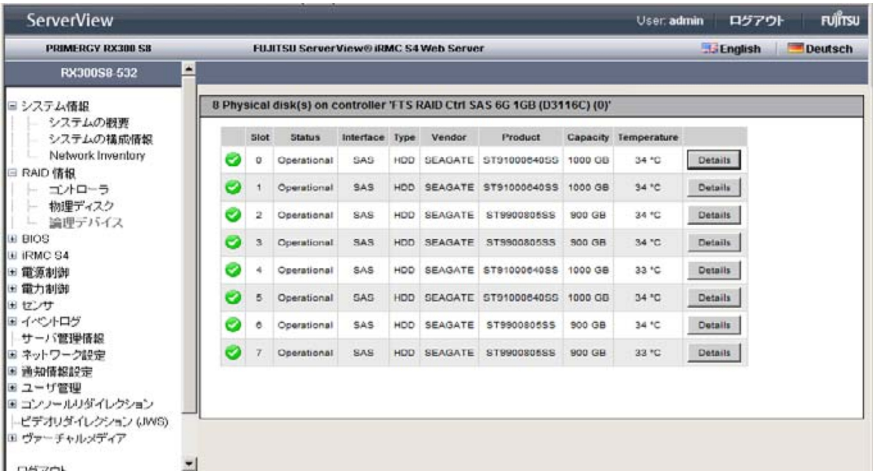


図 65: 「RAID 情報」- 「物理ディスク」ページ

Details

「*Details* 」をクリックすると、対応する RAID 物理ディスクに関する詳細情報が表示される別のページが開きます。

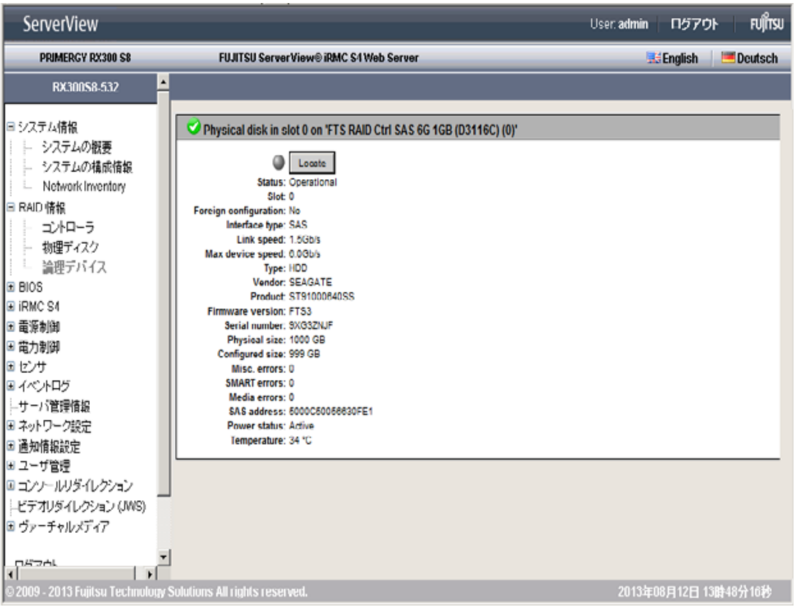


図 66: RAID 物理ディスクの詳細

Locate

RAID 物理ディスクの識別灯がオンになります。

7.5.3 「論理デバイス」- RAID 論理ドライブに関する情報

「*論理デバイス*」ページには、管理対象サーバの各 RAID 論理ドライブに関する情報が表示されます。

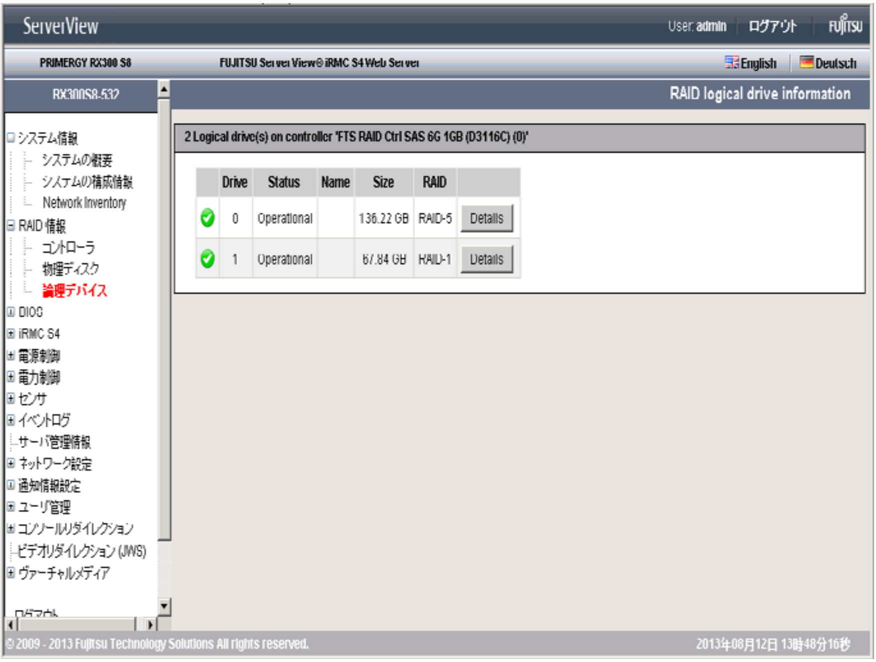


図 67: 「RAID 情報」- 「論理デバイス」ページ

Details

「*Details*」をクリックすると、対応する RAID 論理ドライブに関する詳細情報が表示される別のページが開きます。

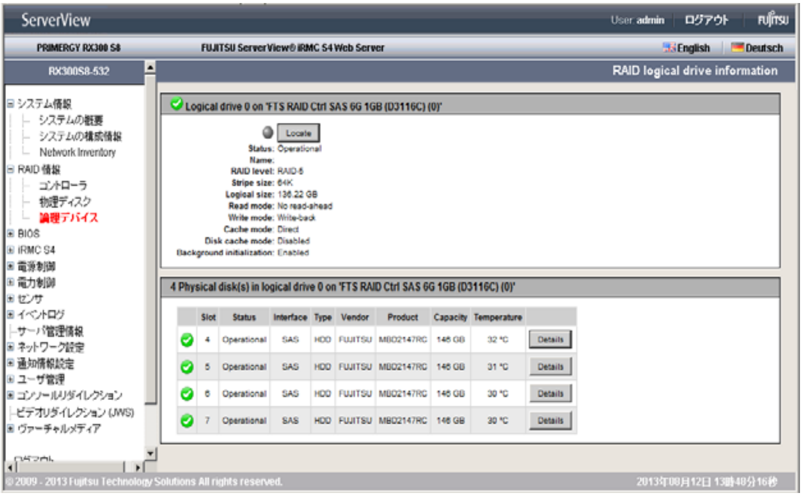


図 68: 論理ドライブの詳細

Locate

論理ドライブがある RAID 物理ディスクの識別灯がオンになります。

7.6 BIOS - BIOS 設定のバックアップ / リストア、BIOS のフラッシュ

「*BIOS*」エントリには、以下のページへのリンクが含まれます。

– 148 ページ の「バックアップ / リストア - BIOS パラメータ設定のファイルへの保存 / ファイルへのリストア」

– 153 ページ の「BIOS アップデート - 「ファイルからアップロード」するか TFTP 経由での BIOS のアップデート」

これらのページは、管理するサーバの BIOS が該当する機能要件を満たす場合のみ表示されます。

7.6.1 バックアップ / リストア - BIOS パラメータ設定のファイルへの保存 / ファイルへのリストア

「*BIOS パラメータ設定のバックアップ / リストア*」ページには以下のオプションがあります。

– 単一の BIOS パラメータを ServerView® WinSCU XML 形式でバックアップし、バックアップをファイルに保存します。

– 単一の BIOS パラメータ設定をファイルから ServerView® WinSCU XML 形式でリストアします。

図 69: 「BIOS パラメータ設定のバックアップ / リストア」ページ

7.6.1.1 単一の BIOS パラメータの ServerView® WinSCU XML 形式でのバックアップ

「*BIOS パラメータを ServerView® WinSCU XML 形式でバックアップ*」グループでは、単一の BIOS パラメータの設定を ServerView® WinSCU XML 形式でバックアップして、バックアップをファイルに保存できます。

図 70: 単一の BIOS パラメータの ServerView® WinSCU XML 形式でのバックアップ

ステータスのバックアップ

現在のバックアッププロセスのステータスを表示します。正常終了すると「作業完了」と表示されます。「*ステータスのバックアップ*」は、バックアップが現在進行中であるか、完了直後のみ表示されます。

このステータスは、「*ステータスのクリア*」ボタンをクリックするとクリアすることができます。このボタンは、ステータスが現在表示されている場合のみ有効です。

ステータスのクリア

「*ステータスのバックアップ*」に表示されるステータス情報をクリアします。このボタンは、「*ステータスのバックアップ*」に現在ステータスが表示されている場合のみ有効です。

バックアップファイル名

デフォルトでは、この入力フィールドは無効です（グレー表示されています）。最初に、iRMC S4 が動的に生成したファイル名が表示されます。

ファイル名の変更

「*バックアップファイル名*」が有効になり、任意のファイル名（*.pre*）を入力できます。

ファイル名の変更

変更したファイル名を保存し、今後、このファイル名がデフォルトで「バックアップファイル名」に表示されます 。

BIOS パラメータのバックアップ要求

単一の BIOS パラメータの ServerView® WinSCU XML 形式でのバックアップを開始します。バックアップ（「*Backup Filename*」フィールドで指定した名前が使用されます）が iRMC S4 にローカルで保存されます。

バックアッププロセスが開始されると、現在のプロセスのステータスが「*ステータスのバックアップ*」に表示されます。

バックアッププロセスについての注意事項

– バックアッププロセス中は、すべてのボタンと入力フィールドが無効です。

– 管理するサーバの電源が切れている場合は、自動的に投入されます。

– サーバの電源が入っている場合は、再起動が必要です。リブートしないと、バックアッププロセスが「Boot Pending」状態のままになります。

– 管理するサーバの電源は、バックアップが完了すると切れます。

ファイルへのバックアップ

BIOS バックアップデータの iRMC S4 のローカルコピーをファイル（<*任意のファイル名* >*.pre*）に保存できるブラウザダイアログが開きます。

このボタンは、単一の BIOS パラメータの ServerView® WinSCU XML 形式でのバックアップが iRMC S4 のローカルストアで使用できる場合のみ表示されます。

7.6.1.2 単一の BIOS パラメータの ServerView® WinSCU XML 形式での復元

「*ServerView® WinSCU XML 形式で保存された BIOS パラメータのリストア*」グループでは、単一の BIOS パラメータの設定を ServerView® WinSCU XML 形式のリストアファイルからリストアできます。

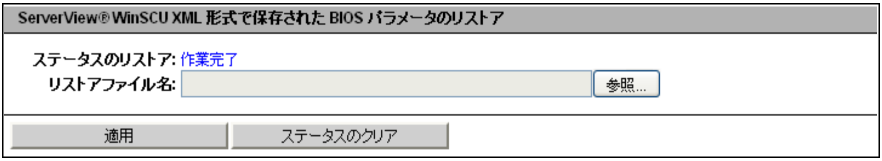


図 71: 単一の BIOS パラメータの ServerView® WinSCU XML 形式での復元

ステータスのリストア

現在のリストアプロセスのステータスを表示します。正常終了すると「作業完了」と表示されます。「*ステータスのリストア*」は、バックアップが現在進行中であるか、完了直後のみ表示されます。

このステータスは、「*ステータスのクリア*」ボタンをクリックするとクリアすることができます。このボタンは、ステータスが現在表示されている場合のみ有効です。

ステータスのクリア

「*ステータスのリストア*」に表示されるステータス情報をクリアします。このボタンは、「*ステータスのリストア*」に現在ステータスが表示されている場合のみ表示されます。

リストアファイル名

入力フィールドをクリックするか、「*参照*」ボタンをクリックすると、ServerView® WinSCU XML 形式の単一の BIOS パラメータのバックアップが含まれるファイル（*.pre*）へ移動できるブラウザダイアログが開きます。

適用

「*リストアファイル名*」フィールドに指定したファイル名に基づいて、単一の BIOS パラメータ設定のリストを開始します。

リストアプロセスが開始されると、現在のプロセスのステータスが「*ステータスのリストア*」に表示されます。

リストアプロセスについての注意事項

– リストアプロセス中は、すべてのボタンと入力フィールドが無効です。

– 管理するサーバの電源が切れている場合は、自動的に投入されます。

– 管理するサーバの電源が入っている場合は、サーバをリブートします。リブートしないと、リストアプロセスが「Boot Pending」状態のままになります。

– 管理するサーバの電源は、リストアが完了すると切れます。

7.6.2 BIOS アップデート - 「ファイルからアップロード」するか TFTP 経由での BIOS のアップデート

「*BIOS アップデート*」ページには、管理するサーバの現在の BIOS 版数が表示され、このページで「ファイルからアップロード」するか TFTP 経由で BIOS をアップデートできます。

> **i** PRIMERGY サーバの適切な BIOS イメージは ServerView Suite DVD に保存されています。また、*http://support.ts.fujitsu.com/com/support/downloads.html* からダウンロードすることもできます。

図 72: 「BIOS アップデート」ページ

BIOS のアップデート（フラッシュ）- イベントと注意事項の指針

以下の概要は、「ファイルからアップロード」する BIOS のアップデートと TFTP 経由での BIOS のアップデートの両方に該当します。

> i この概要に記載される手順を開始する方法の詳細は、この項で後で説明します。

> i すべてのアップデートプロセスの間、現在のアップデートプロセスが「*BIOS TFTP アップデート設定*」ページに表示されます。

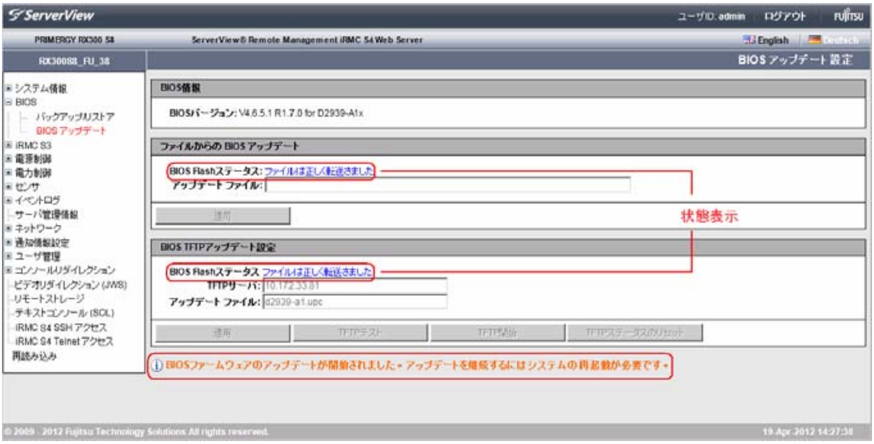


図 73: BIOS アップデート - （TFTP）ダウンロードが正常終了

BIOS のアップデートには、以下の手順が含まれます :

1. 最初の手順で、アップデートファイルをダウンロードします。

   > i アップデートファイルは *UPC* ファイルである必要があります。

   アップデートファイルをダウンロードすると、以下のようになります。

   – サーバの電源が切れている場合は、自動的に電源が投入され、フラッシュプロセスが開始されます。

   – サーバの電源がすでに投入されている場合は、サーバを再起動して、フラッシュプロセスを開始する必要があります。

   > **注意！**
   >
   > BIOS アップデートが現在進行中の場合、サーバの電源を切ったり再起動したり**しないでください**。

2. その後、フラッシュデータがメモリへ転送されます。転送が正常終了すると、ステータス画面が表示されます。
3. 実際のフラッシュプロセスが開始される前に、フラッシュ / アップデートイメージがチェックされます。

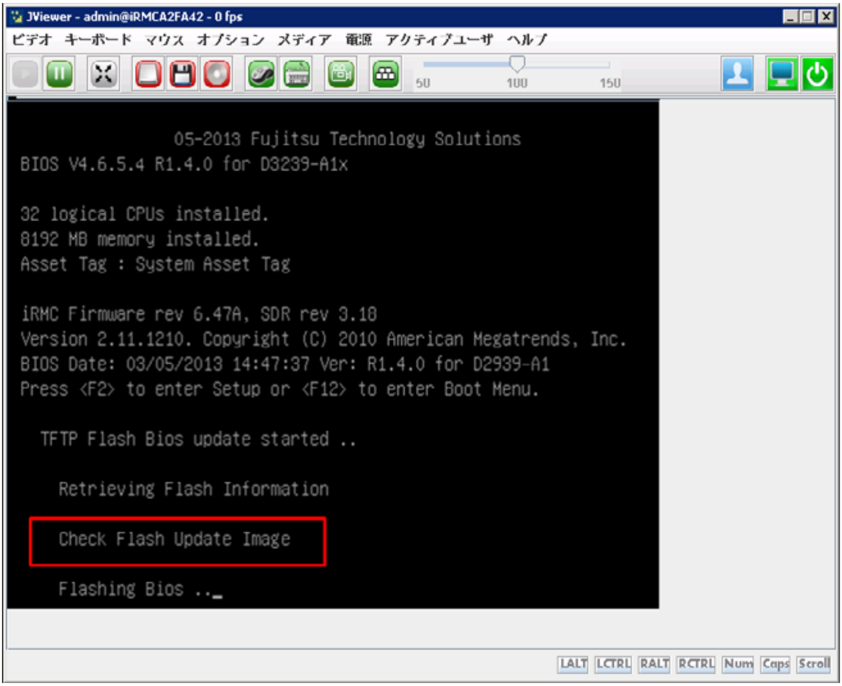


図 74: BIOS アップデート - フラッシュ / アップデートイメージのチェック

4. フラッシュ / アップデートイメージのチェックが正常終了すると、実際のフラッシュプロセスが開始されます。ステータスインジケータに、フラッシュプロセスが何パーセント完了したか表示されます。
5. BIOS アップデートが正常終了すると、サーバの電源が切れます。以下のエントリがシステムイベントログ（SEL）に書き込まれます：

   BIOS TFTP or HTTP/HTTPS flash OK

BIOS 情報

このグループには、管理するサーバの現在の BIOS 版数に関する情報が表示されます。

ファイルからの BIOS アップデート

「*ファイルからの BIOS アップデート*」グループでは、管理するサーバの BIOS をオンラインアップデートできます。この場合、現在の BIOS イメージをファイルに提供する必要があります。

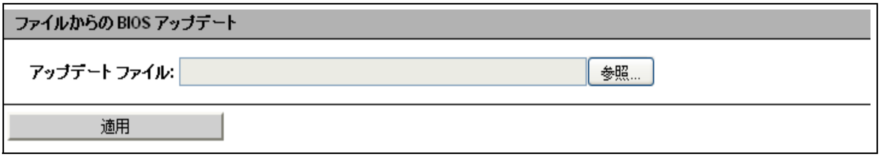


図 75: 「BIOS アップデート」ページ - ファイルからの BIOS アップデート

アップデートファイル

BIOS イメージが格納されるファイル

「*ファイルからの BIOS アップデート*」機能を実行するには、*UPC* 形式のファイルが必要です。

参照

アップデートファイルに移動できるファイルブラウザが開きます。

► 「*適用*」をクリックすると、設定が有効になり、BIOS のフラッシュが開始されます。

注意！

BIOS アップデートが現在進行中の場合、サーバの電源を切ったり再起動したりしないでください。

BIOS TFTP アップデート設定

「*BIOS TFTP アップデート設定*」グループでは、管理するサーバの BIOS をオンラインアップデートできます。この場合、現在の BIOS イメージを TFTP サーバ上のファイルに提供する必要があります。TFTP を起動すると、BIOS がフラッシュされます。

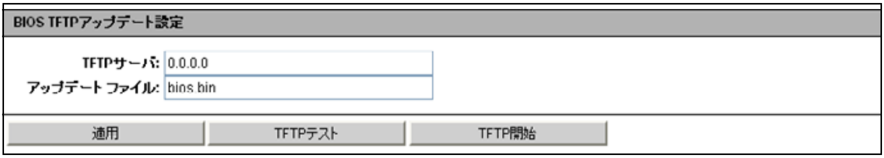


図 76: 「BIOS アップデート」ページ - BIOS TFTP アップデート設定

TFTP サーバ
BIOS イメージを含むファイルが格納される TFTP サーバの IP アドレスまたは DNS 名

アップデートファイル
BIOS イメージが格納されるファイル

「*BIOS TFTP アップデート設定*」機能を実行するには、*UPC* 形式のファイルが必要です。

- 「*適用*」をクリックすると設定が有効になります。
- 「*TFTP テスト*」をクリックすると、TFTP サーバへの接続をテストします。
- 「*TFTP 開始*」をクリックすると、BIOS イメージを含むファイルを TFTP からダウンロードして、BIOS のフラッシュを開始します。

注意！

BIOS アップデートが現在進行中の場合、サーバの電源を切ったり再起動したり**しないでください**。

7.7 iRMC S4 - 情報、ファームウェアおよび認証

「*iRMC S4* 」エントリには、以下のページへのリンクがあります。

– 159 ページ の「「iRMC S4 情報」- iRMC S4 上の情報」
– 166 ページ の「「iRMC S4 ファームウェア設定の保存」- ファームウェア設定の保存」
– 168 ページ の「認証データアップロード - DSA/RSA 証明書および DSA/RSA 秘密鍵のアップロード」
– 175 ページ の「自己署名 RSA 証明書の作成」
– 177 ページ の「iRMC S4 ファームウェアアップデート」

7.7.1 「iRMC S4 情報」- iRMC S4 上の情報

「*iRMC S4 情報*」ページでは、以下のオプションを提供します。

– iRMC S4 のファームウェアおよび SDRR バージョンに関する情報の表示、ファームウェアの選択、ファームウェアイメージのロード、および、iRMC S4 の再起動

– 実行中の iRMC S4 セッションに関する情報の表示

– iRMC S4 へのライセンスキーのアップロード

– iRMC S4 Web インターフェースのレイアウトの設定

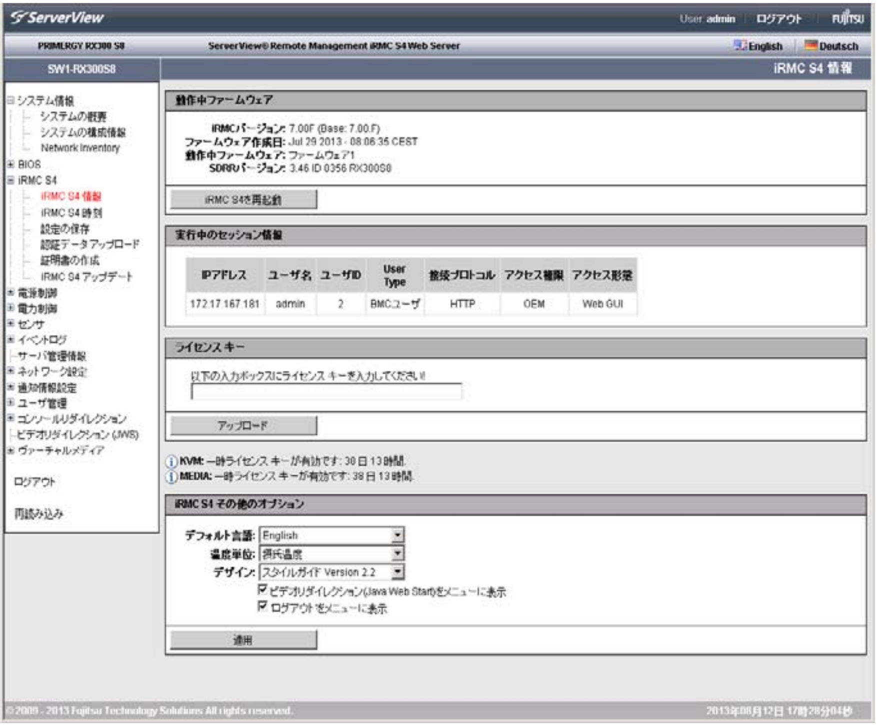


図 77: 「iRMC S4 情報」ページ

動作中ファームウェア

「*動作中ファームウェア*」では、iRMC S4 のファームウェアおよび SDRR バージョンに関する情報の表示と、iRMC S4 の再起動ができます。

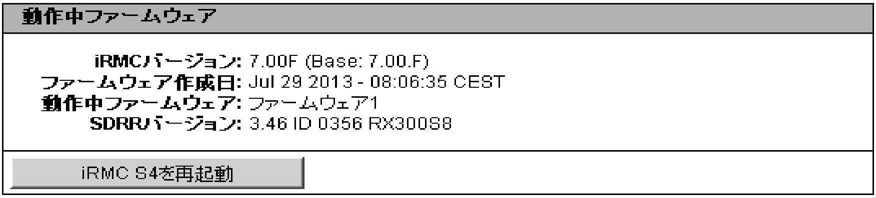


図 78: 「iRMC S4 情報」ページ - 動作中ファオームウェア

iRMC S4 を再起動

iRMC S4 を再起動します。

> **i** 「*iRMC S4 を再起動*」ボタンは、管理対象サーバが BIOS POST フェーズの間は使用できません。

実行中のセッション情報

「*実行中のセッション情報*」グループには、実行中の iRMC S4 セッションがすべて表示されます。

実行中のセッション情報

IPアドレス	ユーザ名	ユーザID	接続プロトコル	アクセス権限	アクセス形態	リモートポート
217.9.101.18	admin	2	HTTP	OEM	Web GUI	0
217.9.101.18	cg_test	7	HTTP	Administrator	Web GUI	4282

図 79: 「iRMC S4 情報」ページ - 実行中のセッション情報

ライセンスキー

「*ライセンスキー*」グループで、iRMC S4 にライセンスキーをアップロードすることができます。

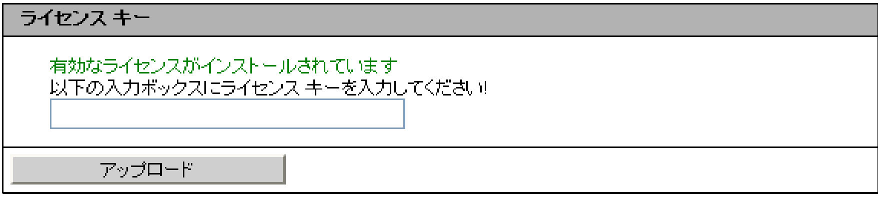


図 80: 「iRMC S4 情報」ページ - ライセンスキー

i iRMC S4 の「*ビデオリダイレクション（AVR）*」機能（288 ページを参照）および「*リモートストレージ」機能*（296 ページを参照）を使用するには、有効なライセンスキーが必要です。

ライセンスキーは購入できます。

アップロード

このボタンをクリックすると、入力フィールドのライセンスキーが iRMC S4 にアップロードされます。

iRMC S4 その他のオプション

「*iRMC S4 その他のオプション*」グループでは、iRMC S4 Web インターフェースのレイアウトを設定できます。

図 81: 「iRMC S4 情報」ページ - iRMC S4 その他のオプション

デフォルト言語

言語の初期設定を行います（ドイツ語 / 英語 / 日本語のいずれか）。次回 iRMC S4 Web インターフェースを呼び出す際に有効になります。

温度単位

iRMC S4 Web インターフェースで表示する温度の単位（摂氏 / 華氏）を設定します。この設定は現在のセッションに適用され、次回 iRMC S4 Web インターフェースを呼び出す際に有効になります。

デザイン

iRMC S4 Web インターフェースを表示するためのカラースキーマを設定します。この設定は現在のセッションに適用され、次回 iRMC S4 Web インターフェースを呼び出す際に有効になります。

ビデオリダイレクション（Java Web Start）をメニューに表示

「*ビデオリダイレクション（JWS）*」リンクをナビゲーションエリアに追加します。このリンクを使用して直接ビデオリダイレクション（Java Web Start）を開始できます（294 ページ の「ビデオリダイレクション - AVR の開始」を参照）。

' ログアウト ' をメニューに表示

このオプションは、「iRMC S4 情報」ページが「*スタイルガイド Version 2.2*」のデザインで表示されている場合のみ使用できます。

「*ログアウト*」リンクをナビゲーションエリアに追加します。このリンクを使用してナビゲーションエリアでログアウトできます。

7.7.2 「iRMC S4 時刻」- iRMC S4 の時刻オプション

「*iRMC S4 時刻*」ページでは、iRMC S4 の時刻に関する設定を行うことができます。

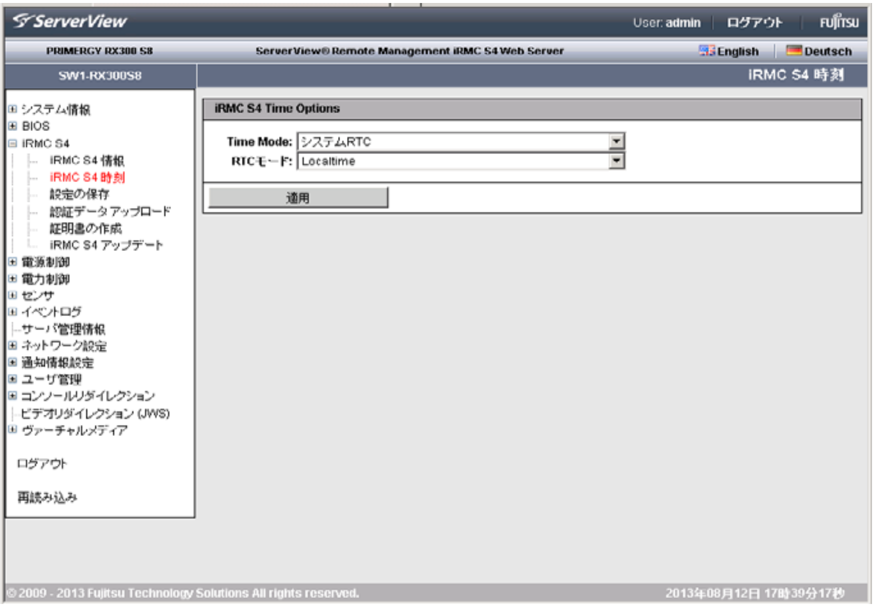


図 82: 「iRMC S4 時刻」ページ

iRMC S4 Time Options

「*iRMC S4 Time Options*」グループでは、iRMC S4 の時刻に関する設定を行うことができます。

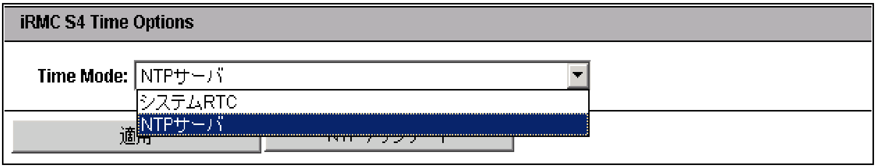


図 83: 「iRMC S4 時刻」ページ - iRMC S4 Time Options

Time Mode

ここでは、iRMC S4 の時刻設定を管理対象サーバから取得するか、NTP サーバから取得するかを選択できます。

システム RTC

iRMC S4 は、管理対象サーバのシステムクロックから時刻を取得します。

NTP サーバ

iRMC S4 は、ネットワークタイムプロトコル（NTP）を使用して独自の時刻を参照時刻ソースとして動作する NTP サーバと同期します。

このオプションが有効な場合、追加のグループの「*NTP (Network Time Protocol) Configuration*」グループが表示され、必要な NTP 設定を行うことができます（下記参照）。

RTC モード

ここでは、今後、iRMC S4 の時刻を UTC（協定世界時）形式で表示するか、ローカルタイム形式で表示するかを選択できます。

UTC（Universal Time Coordinated）

iRMC S4 の時刻を UTC（協定世界時）形式で表示します。

このオプションが有効な場合、追加のグループの「*タイムゾーン構成*」グループが表示され、目的のタイムゾーンを選択できます（下記参照）。

Localtime

iRMC S4 の時刻をローカルタイム形式で表示します。

NTP（Network Time Protocol）Configuration

「*NTP（Network Time Protocol）Configuration*」グループで必要な設定を行うには、「*iRMC S4 Time Options*」グループの「*NTP サーバ*」オプションが有効である必要があります。

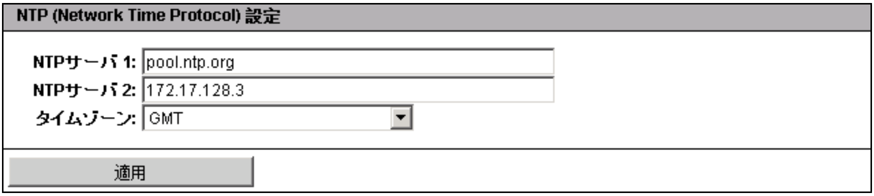


図 84: 「iRMC S4 情報」ページ - NTP(Network Time Protocol) 設定

NTP サーバ 1
: プライマリ NTP サーバの IP アドレスまたは DNS 名。

NTP サーバ 2
: セカンダリ NTP サーバの IP アドレスまたは DNS 名。

タイムゾーン
: PRIMERGY サーバのある場所に対応する「*タイムゾーン*」を設定します。

7.7.3 「iRMC S4 ファームウェア設定の保存」- ファームウェア設定の保存

「*iRMC S4 ファームウェア設定の保存*」ページでは、現在のファームウェア設定および iRMC S4 の他の多くの設定をファイルに保存できます。また、ファームウェア設定を iRMC S4 に再びアップロードすることもできます。

> **i** ユーザ設定を保存する場合（*「ユーザ設定」*）、「*ユーザアカウント変更権限*」が必要です。その他の場合はすべて、「*iRMC S4 設定の構成*」権限で十分です。

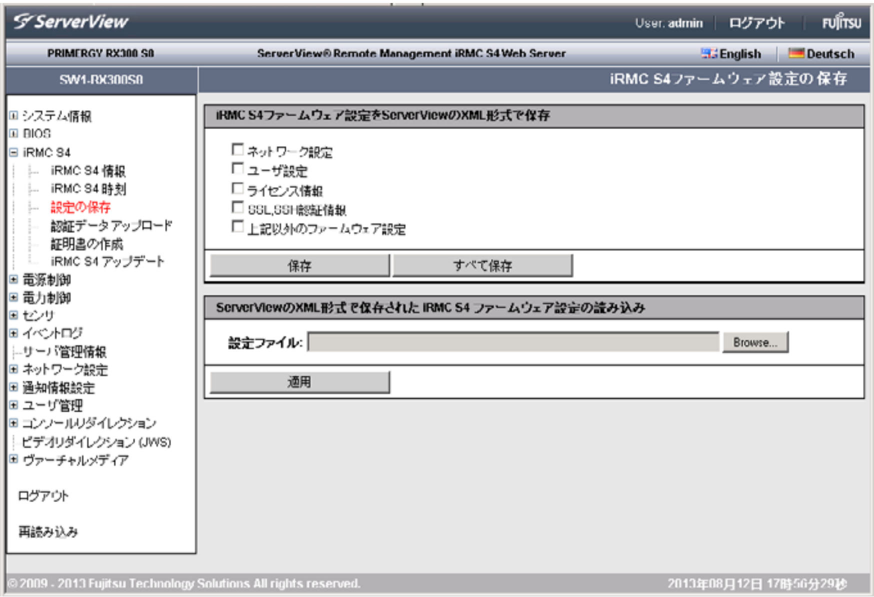


図 85: 「iRMC S4 ファームウェア設定の保存」ページ

iRMC S4 ファームウェア設定の保存 ...

データは iRMC S4 から、それぞれ選択するオプションに応じた論理セクションにエクスポートされます。

オプション「*上記以外のファームウェア設定*」を選択すると、ファームウェアは、まだエクスポートされていない現行のすべての ConfigSpace 値とその他のセクションをエクスポートします。新規に実装された値は、自動的に新しいファームウェアバージョンにエクスポートされます。

保存

選択した設定を保存するには、「*保存*」をクリックします。

すべて保存

すべての設定を保存するには、「*すべて保存*」をクリックします。

ServerView の XML 形式で保存された iRMC S4 ファームウェア設定の読み込み

設定ファイル

ServerView® WinSCU の XML 形式の設定ファイル（デフォルト：*iRMC_S4_settings.bin*）。このファイルからファームウェア設定を iRMC S4 に読み込みます。

参照

設定ファイルに移動できるファイルブラウザが開きます。

7.7.4 認証データアップロード - DSA/RSA 証明書および DSA/RSA 秘密鍵のアップロード

「*認証データアップロード*」ページでは、認証機関（CA）からの署名付 X.509 DSA/RSA 証明書（SSL）、または DSA/RSA 秘密鍵（SSH）を iRMC S4 にアップロードすることができます。

i iRMC S4 は、あらかじめ定義されたサーバ認証証明書（規定の証明書）を提供します。安全な SSL/SSH で、iRMC S4 に接続したい場合、認証機関（CA）からの署名付認証証明書にできるだけ早く置き換えることを推奨します。

i X.509 DSA/RSA 認証および DSA/RSA 秘密鍵の入力フォーマット :

X.509 DSA/RSA 証明書も RSA/DSA も PEM エンコード形式（ASCII/Base64）に対応してる必要があります。

図 86: 「認証データアップロード」ページ

現在有効な（CA）DSA/RSA 証明書の表示

- 「*証明書の情報とリストア*」グループで「*Web 証明書を表示*」をクリックすると、有効な SSH/SSL 証明書が表示されます。
- 「*証明書の情報とリストア*」グループで「*認証局の証明書を表示*」をクリックすると、現在の有効な認証局証明書が表示されます。

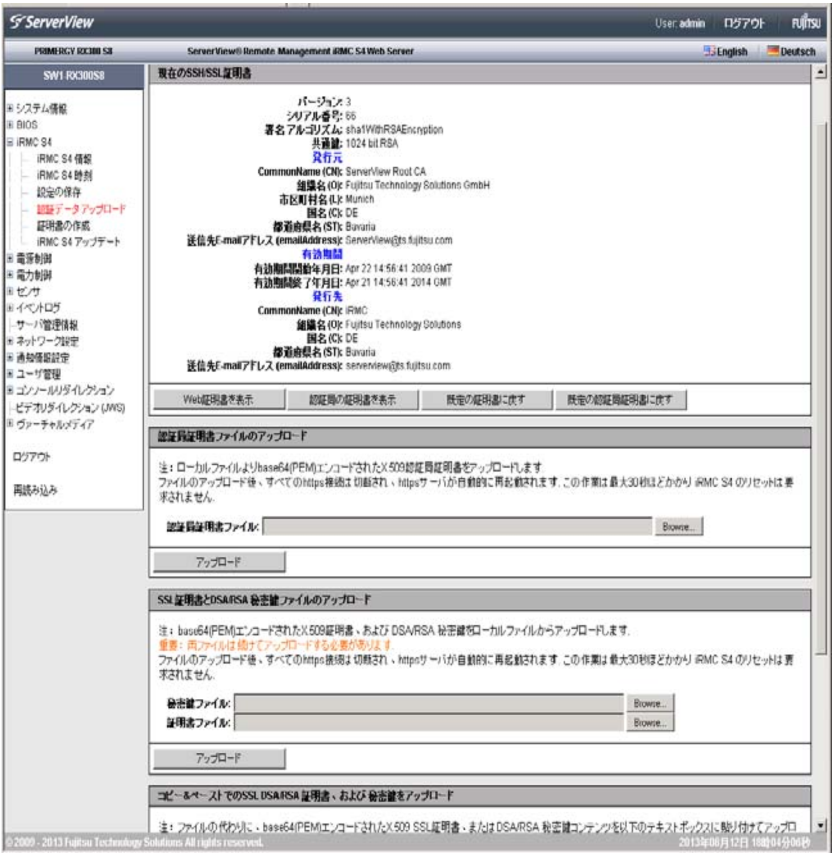


図 87: 「認証データアップロード」ページ - 現在有効な SSL/SSH 証明書の表示

規定の証明書および規定の認証局証明書のリストア

- 「*証明書の情報とリストア*」グループで「*規定の証明書に戻す*」をクリックすると、確認後に規定の証明書がファームウェアに設定されます。
- 「*証明書の情報とリストア*」グループで「*規定の認証局証明書に戻す*」をクリックすると、確認後に規定の認証局証明書がファームウェアに設定されます。

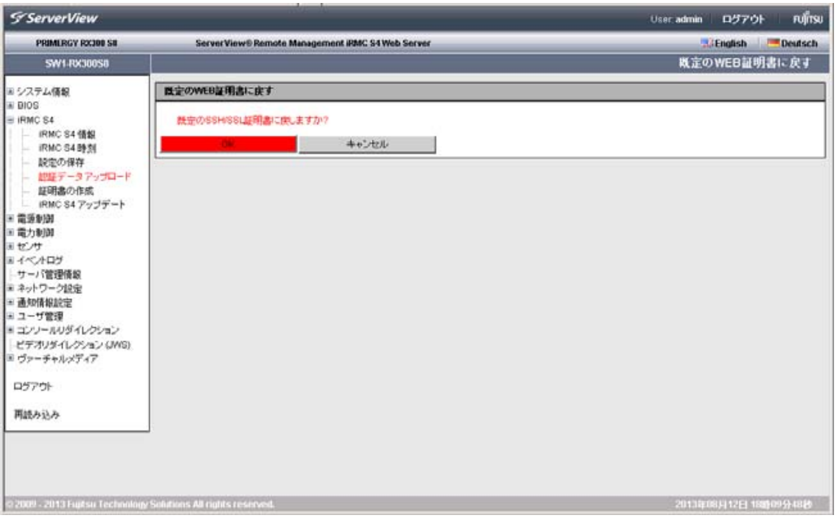


図 88: 「認証データアップロード」ページ - 規定の認証局証明書に戻す

認証局証明書のアップロード

「*認証局証明書ファイルのアップロード*」グループを使用して、認証局証明書をローカルファイルからアップロードすることができます。

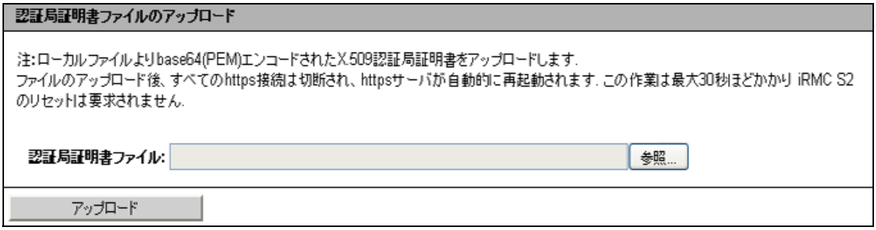


図 89: 「認証データアップロード」ページ - 認証局証明書ファイルのアップロード

次の手順に従います。

- ▶ 認証局証明書を管理対象サーバのローカルファイルに保存します。
- ▶ このファイルを「*認証局証明書ファイル*」で指定するには、「*参照*」ボタンをクリックして認証局証明書を含むファイルを選択します。
- ▶ 「*アップロード*」ボタンをクリックして、証明書または秘密鍵を iRMC S4 にアップロードします。

  i 証明書または秘密鍵をアップロードすると、既存の HTTPS 接続はすべて閉じられ、HTTPS サーバは自動的に再起動します。このプロセスは最大 30 秒ほどかかることがあります。

  iRMC S4 を明示的にリセットする必要は**ありません**。

- ▶ 「*認証局証明書を表示*」ボタンをクリックして、証明書のアップロードが成功していることを確認してください。

SSL 証明書と DSA/RSA 秘密鍵ファイルのアップロード

*「SSL 証明書と DSA/RSA 秘密鍵ファイルのアップロード」*グループを使用してアップロードします。

> **i** 秘密鍵と証明書は、iRMC S4 に同時にアップロードします。

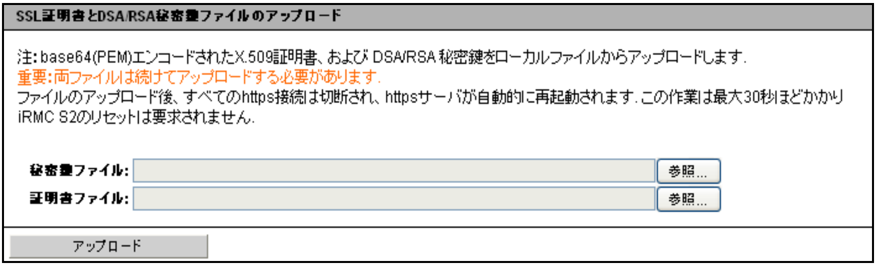


図 90: 「認証データアップロード」ページ - SSL 証明書と DSA/RSA 秘密鍵ファイルのアップロード

次の手順に従います。

- ▶ X.509 DSA/RSA（SSL）証明書と DSA/RSA 秘密鍵を管理対象サーバ上の対応するローカルファイルに保存します。
- ▶ 「*秘密鍵ファイル*」と「*証明書ファイル*」を指定するには、「*参照*」ボタンをクリックして秘密鍵または証明書を含むファイルを選択します。
- ▶ 「*アップロード*」ボタンをクリックして、証明書または秘密鍵を iRMC S4 にアップロードします。

  > **i** 証明書と秘密鍵をアップロードすると、既存の HTTPS 接続はすべて閉じられ、HTTPS サーバは自動的に再起動します。このプロセスは最大 30 秒ほどかかることがあります。
  >
  > iRMC S4 を明示的にリセットする必要はありません。

- ▶ 「*認証局証明書を表示*」ボタンをクリックして、証明書のアップロードが成功していることを確認してください。

DSA/RSA 証明書 /DSARSA 秘密鍵の直接入力

「*コピー＆ペーストでの SSL DSA/RSA 証明書、および DSA/RSA 秘密鍵をアップロード*」グループを使用して行います。

> **i** この方法を使用して認証局証明書を iRMC S4 にアップロード**しないでください**。認証局証明書は必ずファイルを使用してアップロードしてください（173 ページ を参照）。

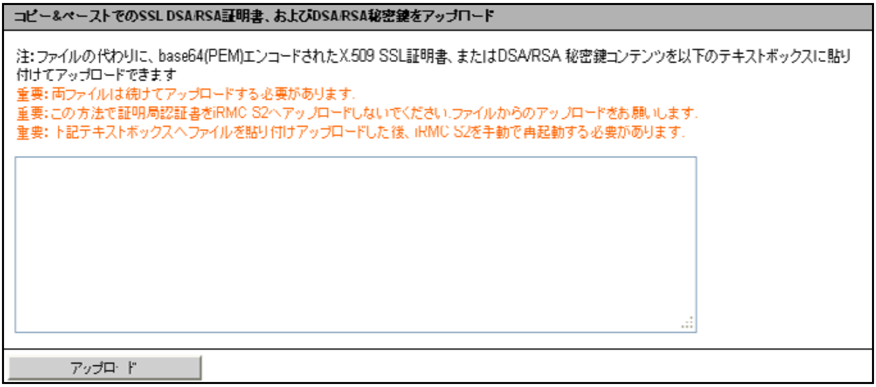


図 91: 「認証データアップロード」ページ - コピー & ペーストでの SSL DSA/RSA 証明書、および 秘密鍵をアップロード

次の手順に従います。

► 入力エリアに、X.509 DSA 証明書**または** DSA 秘密鍵をコピーします。

> **i** 同じアップロードで証明書と秘密鍵を同時に入力することはできません。

► 「*アップロード*」ボタンをクリックして、証明書または秘密鍵を iRMC S4 にアップロードします。

► [iRMC S4 を再起動]（323 ページ の「サービスプロセッサ - IP パラメータ、識別灯、iRMC S4 リセット」の項を参照）を使用して iRMC S4 をリセットします。

> **i** これは、iRMC S4 にアップロードした証明書および秘密鍵を有効にするために必要です。

► 「*認証局証明書を表示*」ボタンをクリックして、証明書のアップロードが成功していることを確認してください。

7.7.5 自己署名 RSA 証明書の作成

「*自己署名 RSA 証明書の作成*」ページを使用して自己署名証明書を作成できます。

図 92: 「自己署名 RSA 証明書の作成」ページ

証明書の情報とリストア

「*証明書の情報とリストア*」グループを使用して、現在有効な DSA/RSA 証明書の表示や、規定の RSA/DSA 証明書のリストアができます。

Web 証明書を表示
このボタンを使用して、現在有効な DSA/RSA 証明書を表示することができます。

規定の証明書に戻す
このボタンを使用して、確定後、ファームウェアに提供された既定の証明書を復元することができます。

証明書の作成

次の手順で自己署名入り証明書を作成することができます。

- 「*証明書の作成*」に詳細な必要項目を入力してください。
- 「*作成*」をクリックして、証明書を作成してください。

i 新しい証明書を生成すると、既存の HTTPS 接続がすべて切断され、HTTPS サーバが自動的に再起動します。キーの長さによって、最大 5 分ほどかかることがあります。

iRMC S4 を明示的にリセットする必要は**ありません**。

7.7.6 iRMC S4 ファームウェアアップデート

「*iRMC S4 ファームウェアアップデート*」ページを使用して、iRMC S4 ファームウェアをオンラインでアップデートすることができます。そのためには、ローカルでリモートワークステーション上に、または TFTP サーバ上に現在のファームウェアイメージをアップロードする必要があります。

ここでは、iRMC S4 ファームウェアおよびファームウェア選択に関する情報も参照してください。

図 93: 「iRMC S4 ファームウェアアップデート」ページ

ファームウェア情報

「*ファームウェア情報*」では、iRMC S4 のファームウェアバージョンおよび SDRR バージョンに関する情報の表示と、ファームウェアセレクタの設定ができます。

図 94: 「iRMC S4 ファームウェアアップデート」- ファームウェア情報

ファームウェア変更

ファームウェアセレクタを使用して、次回 iRMC S4 を再起動したときに、有効にするファームウェアを選択します。

以下のオプションがあります。

– *自動 - 版数が新しいファームウェアを使用*

最新バージョンのファームウェアイメージが自動的に選択されます。

– *ファームウェア 1*

低いファームウェアイメージが選択されます。

– *ファームウェア 2*

高いファームウェアイメージが選択されます。

– *版数が古いファームウェアを選択*

最も古いバージョンのファームウェアイメージが選択されます。

– *書込日が新しいファームウェア*

更新時期の最も新しいファームウェアイメージが選択されます。

– *書込日が古いファームウェア*

更新時期の最も古いファームウェアイメージが選択されます。

適用

「*適用*」をクリックして、「*ファームウェア変更*」で設定したオプションをファームウェアに設定します。

ファイルからのファームウェアアップデート

「*ファイルからのファームウェアアップデート*」ページを使用して、iRMC S4 ファームウェアをオンラインでアップデートできます。そのためには、リモートワークステーション上のファイルに現在のファームウェアイメージを保存する必要があります。

PRIMERGY サーバの適切なファームウェアイメージは ServerView Suite DVD に保存されています。また、*http://support.ts.fujitsu.com/com/support/downloads.html* からダウンロードすることもできます。

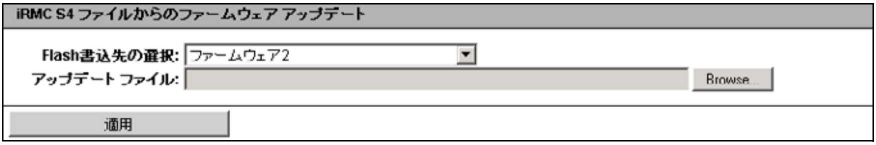


図 95: 「iRMC S4 ファームウェアアップデート」- ファイルからのファームウェアアップデート

Flash 書込先の選択

アップデートする iRMC ファームウェアを指定します。

以下のオプションがあります。

– *自動－不活性なファームウェア*

  アクティブでないファームウェアが自動的に選択されます。

– *ファームウェア 1*

  低ファームウェアイメージ（ファームウェアイメージ 1）が選択されます。

– *ファームウェア 2*

  高ファームウェアイメージ（ファームウェアイメージ 2）が選択されます。

アップデートファイル

ファームウェアイメージが保存されたファイルを指定します。

> **i** ファームウェアバージョンおよび SDRR バージョンで構成される完全なファームウェアイメージ（例 : *RX30S8_07.01F_sdr03.47.bin*）のみアップデートできます。

参照

アップデートファイルに移動できるファイルブラウザが開きます。

▶ *「適用」*ボタンをクリックして設定を有効にし、iRMC S4 ファームウェアのアップデートを開始します。

iRMC S4 TFTP 設定

「*iRMC S4 TFTP 設定*」グループでは、オンラインで iRMC S4 ファームウェアをアップデートできます。そのためには、TFTP サーバ上のファイルにファームウェアイメージを保存する必要があります。

PRIMERGY サーバの適切なファームウェアイメージは ServerView Suite DVD に保存されています。また、*http://support.ts.fujitsu.com/com/support/downloads.html* からダウンロードすることもできます。

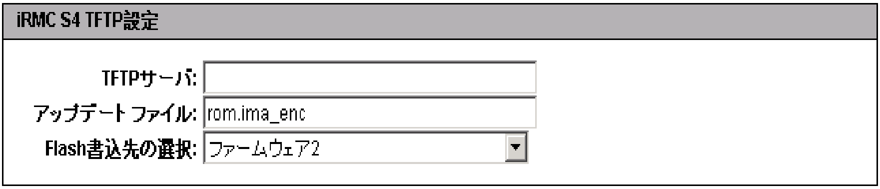


図 96: 「iRMC S4 ファームウェアアップデート」ページ - 「iRMC S4 TFTP 設定」

TFTP サーバ

ファームウェアイメージのファイルが保存される TFTP サーバの IP address または DNS 名。

アップデートファイル

ファームウェアイメージが保存されたファイルを指定します。

> **i** 完全なファームウェアイメージ（例 : *RX30S8_07.01F_sdr03.47.bin*）のみアップデートできます。

Flash 書込先の選択

アップデートする iRMC ファームウェアを指定します。

以下のオプションがあります。

– *自動－不活性なファームウェア*

アクティブでないファームウェアが自動的に選択されます。

– *Low Firmware Image*

低ファームウェアイメージ（ファームウェアイメージ 1）が選択されます。

– *High Firmware Image*

高ファームウェアイメージ（ファームウェアイメージ 2）が選択されます。

► 「*適用*」をクリックすると設定が有効になります。

► 「*TFTP テスト*」をクリックすると、TFTP サーバへの接続をテストします。

► 「*TFTP 開始*」ボタンクリックして、TFTP サーバからファームウェアを含むファイルをダウンロードし、S4 ファームウェアのアップデートを開始します。

7.8 電源制御

「*電源制御*」エントリには、PRIMERGY サーバの電源管理ページへのリンクが含まれます。

– 183 ページ の「電源投入 / 切断 －サーバの自動電源投入 / 切断」

– 187 ページ の「電源制御オプション - サーバの電源制御の構成」

– 190 ページ の「電源装置情報 - 電源装置および FRU コンポーネントの IDPROM データ」

7.8.1 電源投入 / 切断 －サーバの自動電源投入 / 切断

「*Power On/Off*」ページでは、管理サーバの電源オン / オフを行います。サーバの現在の電源状態が表示され、次回の起動時のサーバの設定も行うことができます。

図 97: 「Power On/Off」ページ

電源状態概要

「*電源状態概要*」グループには、サーバの現在の電源状態の情報、および最後のサーバの電源オン / オフの理由が表示されます。また、サーバの電源が投入されてからの経過時間（月、日、分）も表示されます。

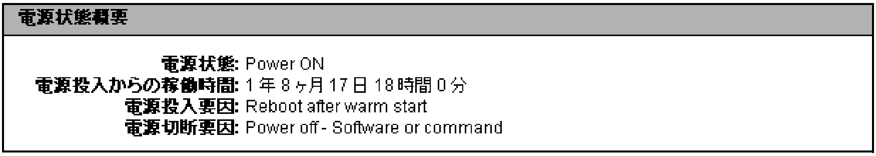


図 98: 「Power On/Off」ページ - 電源状態概要

起動オプション

「*起動オプション*」グループには、**次回**起動時のシステム構成を設定することができます。BIOS がシステムの起動プロセスに割り込んだ場合か、POST フェーズでエラーが発生した場合かを設定できます。

i ここで設定するオプションは、次回の起動時にのみ有効になります。その後、初期設定が再び適用されます。

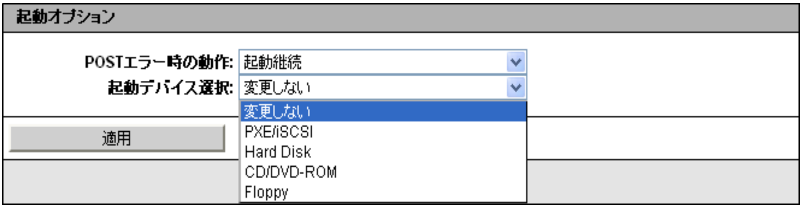


図 99: 「Power On/Off」ページ - 起動オプション

POST エラー時の動作

必要な BIOS の動作を指定します。

継続稼働

POST フェーズ中にエラーが発生しても、起動プロセスを継続します。

起動停止

POST フェーズ中にエラーが発生した場合、起動プロセスを停止します。

起動デバイス選択

起動するストレージメディア。

以下のオプションを選択できます。

- 「*変更しない*」: システムを前回と同じストレージメディアから起動します。
- 「*PXE/iSCSI*」: システムをネットワーク上の PXE あるいは iSCSI から起動します。
- 「*Hard Disk*」: システムをハードディスクから起動します。
- 「*CD/DVD-ROM*」: システムを CD/DVD から起動します。
- 「*Floppy*」: システムをフロッピーディスクから起動します。
- 「BIOS セットアップ」: 起動時にシステムが BIOS セットアップに入ります。

次回起動時のみ適用する

設定は、次の起動時にのみ適用されます。

► 「*適用*」をクリックすると設定が有効になります。

電源制御 - サーバの電源投入・切断 / サーバの再起動

「*電源制御*」グループを使用して、サーバの電源投入 / 切断や、サーバの再起動を行うことができます。

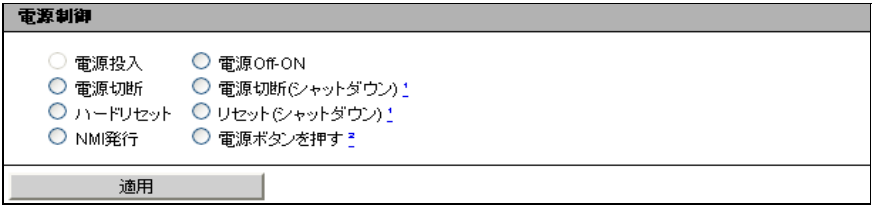


図 100: 「Power On/Off」ページ、再起動（サーバ電源投入）

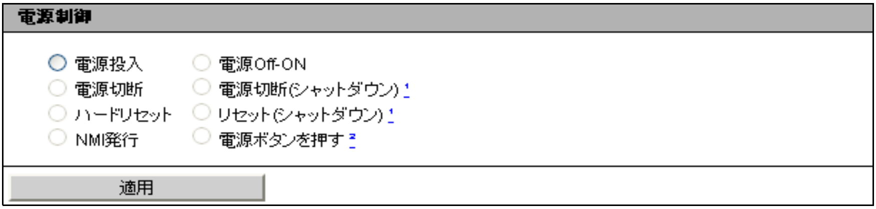


図 101: 「Power On/Off」ページ、再起動（サーバ電源切断）

電源投入

サーバの電源を投入します。

電源切断

オペレーティングシステムの状態にかかわらず、サーバの電源を切断します。

ハードリセット

オペレーティングシステムの状態にかかわらず、サーバを完全に再起動します（コールドスタート）。

NMI 発行

マスク不可能な割り込み（NMI：Non-Maskable Interrupt）を初期化します。NMI は、システムの標準の割り込みマスクテクノロジで無視できるプロセッサ割り込みです。

電源ボタンを押す

インストールされているオペレーティングシステムと設定されている動作に依存して、電源オフボタンを短く押してさまざまな動作をトリガできます。これらの動作では、コンピュータのシャットダウンや、スタンバイモードまたはスリープモードへの切り替えができます。

パワーサイクル

サーバの電源が完全に切断され、設定した時間の経過後、再び投入されます。この時間は、「*ASR&R オプション*」グループの「*パワーサイクル間隔*」フィールドで設定できます（225 ページを参照）。

電源切断（シャットダウン）

グレースフルシャットダウンし、電源を切断します。
このオプションは、ServerView エージェントがインストールされていて、かつ、iRMC S4 にサインオンして「接続中」の場合のみ使用できます。

リセット（シャットダウン）

正常にシャットダウンして、再起動します。
このオプションは、ServerView エージェントがインストールされていて、かつ、iRMC S4 にサインオンして「接続中」の場合のみ使用できます。

► 「*適用*」ボタンをクリックして目的の動作を開始します。

7.8.2 電源制御オプション - サーバの電源制御の構成

「*電源制御オプション*」ページを使用して、停電後のサーバ動作およびサーバの電源オン / オフ時刻の設定を行うことができます。

図 102: 「電源制御オプション」ページ

電源復旧時動作設定 - 停電後のサーバ動作の指定

「*電源復旧時動作設定*」グループを使用して、停電後のサーバの電源管理動作を指定できます。

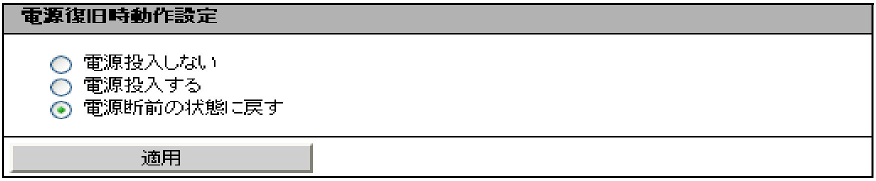


図 103: 「電源制御オプション」ページ - 電源復旧時動作設定

電源投入しない
　　停電後、サーバの電源を常にオフのままにします。

電源投入する
　　停電後、サーバの電源を常にオンにします。

電源切断前の状態に戻す
　　停電前のサーバの電源オン / オフ状態に復旧します。

► 「*適用*」をクリックすると設定が有効になります。

設定した動作は、停電後に実行されます。

自動電源投入 / 切断時刻設定 - サーバの自動電源投入 / 切断時刻設定

「*自動電源投入 / 切断時刻設定*」グループの入力フィールドを使用して、特定曜日あるいは特定時間のサーバの自動電源投入 / 切断時刻を設定することができます。

> i 「*毎日*」フィールドの指定が最優先です。

「*Trap*」フィールドを使用して、iRMC S4 が予定された管理対象サーバの電源投入 / 切断前に SNMP トラップを管理コンソールに送信したりするかどうかを設定することもできます。その場合、このイベントの前に何分行うかを指定できます。値に「0」を設定すると、トラップは送信されません。

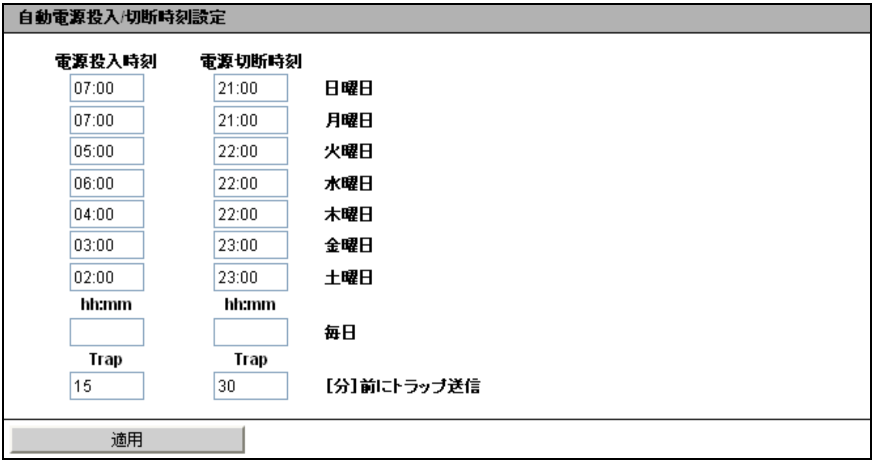


図 104: 「電源制御オプション」ページ - 自動電源投入 / 切断時刻設定

7.8.3 電源装置情報 - 電源装置および FRU コンポーネントの IDPROM データ

「*電源装置情報*」ページには、電源装置に関する情報と、サーバの FRU の IDPROM データが表示されます。

「*CSS 対象*」列には、各コンポーネントの CSS（**C**ustomer **S**elf **S**ervice）機能のサポートの有無が示されます。

図 105: 「電源装置情報」ページ

7.9 電力制御

「*電力制御*」エントリには、管理対象サーバの消費電力の監視と制御に関するページのリンクが含まれます。

– 192 ページ の「消費電力制御 - サーバの消費電力制御」

– 187 ページ の「電源制御オプション - サーバの電源制御の構成」（iRMC S4 が搭載されるすべてのサーバに表示されるわけではありません。）

– 199 ページ の「消費電力モニタリング履歴 - 消費電力の表示」（iRMC S4 が搭載されるすべてのサーバに表示されるわけではありません。）

7.9.1 消費電力制御 - サーバの消費電力制御

「*消費電力制御*」ページでは、iRMC S4 が PRIMERGY サーバの消費電力制御に使用するモードを指定できます。

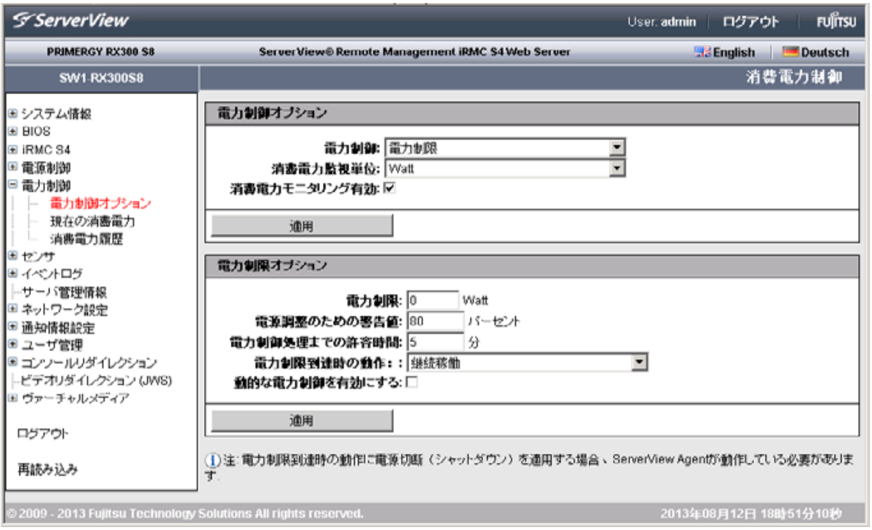


図 106: 「消費電力制御」ページ

前提条件：

消費電力制御を行うには以下の条件を満たす必要があります。

– PRIMERGY 管理対象サーバが、この機能をサポートしている必要があります。

– 「*Enhanced Speed Step*」または「*Processor Power Management*」オプションが、BIOS セットアップの「*Advanced*」メニューで有効である必要があります。

「*電源制御オプション*」グループまたは「*電力制御スケジュール*」で電力制御を「電力制限」に設定した場合、「*電力制限オプション*」グループも表示されます（194 ページを参照）。

電力制御オプション

「*電力制御オプション*」グループでは、電力制御モードを選択し、消費電力の時間的経過を監視するかどうかを指定できます。

電力制御

管理対象サーバの消費電力制御モードは以下の通りです。

– O/S によるコントロール :

消費電力は、管理対象サーバのオペレーティングシステムによって制御されます。

– *省電力動作* :

iRMC S4 は、最小消費電力を達成するようにサーバを制御します。この場合、サーバのパフォーマンスは常に理想的であるとは言えません。

– *スケジュール* :

iRMC S4 は、スケジュールに従って消費電力を制御します（194 ページ の「電力制御スケジュール」を参照）。

– *電力制限* :

「*電力制限オプション*」グループが表示されます（196 ページ の「電力制限オプション」を参照）。

消費電力監視単位

消費電力を表示する単位は以下の通りです :

– *Watt*

– *BTU/h*（BTU/ 時（British Thermal Unit/ 時、1 BTU/ 時は 0.293 ワットに相当します。）

消費電力モニタリング有効

このオプションを有効にした場合、消費電力は連続的に監視されます。

> **i** この設定は、電力監視をサポートする PRIMERGY サーバにのみ有効です。

▶ 「*適用*」をクリックすると設定が有効になります。

電力制御スケジュール

「*電力制御スケジュール*」グループでは、iRMC S4 が管理対象サーバの消費電力を制御するために使用する詳細なスケジュールとモード（*O/S controlled*、*最小消費電力* , *電力制限*) を指定できます。

> **i** 「*電力制御スケジュール*」グループは、「*電力制御オプション*」グループの電力制御モードを「*スケジュール*」に設定した場合のみ表示されます。

> **i** 電力制御スケジュールモードの設定は、「*Enhanced Speed Step*」オプションが BIOS セットアップで有効であることが前提です。有効でない場合、その旨のメッセージが表示されます。
>
> 「Enhanced Speed Step」オプションが有効であるにもかかわらずこのメッセージが表示される場合、以下の理由が考えられます。
>
> – サーバの CPU （低電力 CPU）が、電力制御スケジュールをサポートしていない。
>
> – システムが、現在 BIOS POST フェーズである。

図 107: 「消費電力制御」ページ - 電力制御スケジュール

時刻 1

iRMC S4 が、「*モード 1*」で、指定する曜日に消費電力制御を開始する時刻 [hh : ss]。

時刻 2

iRMC S4 が、「*モード 2*」で、指定する曜日に消費電力制御を開始する時刻 [hh : ss]。

モード 1

iRMC S4 が、「*時刻 1*」で、指定する曜日に使用するよう設定された電力制御モード。

モード 2

iRMC S4 が、「*時刻 2*」で、指定する曜日に使用するよう設定された電力制御モード。

i 「*時刻 1*」<「*時刻 2*」となるように設定してください。そうでない場合、「*モード 2*」に指定した電力制御モードは次の週の該当する曜日の「*時刻 2*」でしか有効になりません。

i 「*毎日*」フィールドの指定が最優先です。

► 「*適用*」をクリックすると設定が有効になります。

> **i** Server Configuration Manager を使用して電力制御スケジュールを設定することもできます（333 ページ の「Server Configuration Manager を使用した iRMC S4 の設定」の章を参照）。

電力制限オプション

「*電力制限オプション*」グループは、次の場合に表示されます。

– 電力制御モードの「*電力制限*」が選択され、「*電力制御オプション*」グループで有効である場合。

– 「*電力制御オプション*」グループで電力制御モードの「*スケジュール*」が有効で、「電力制御スケジュール」グループで電力制御モードの「*電力制限*」が少なくとも一度有効である場合。

この電力制限は、この電力制御モードが「*消費電力制御スケジュール*」グループで有効なすべての期間に適用されます。

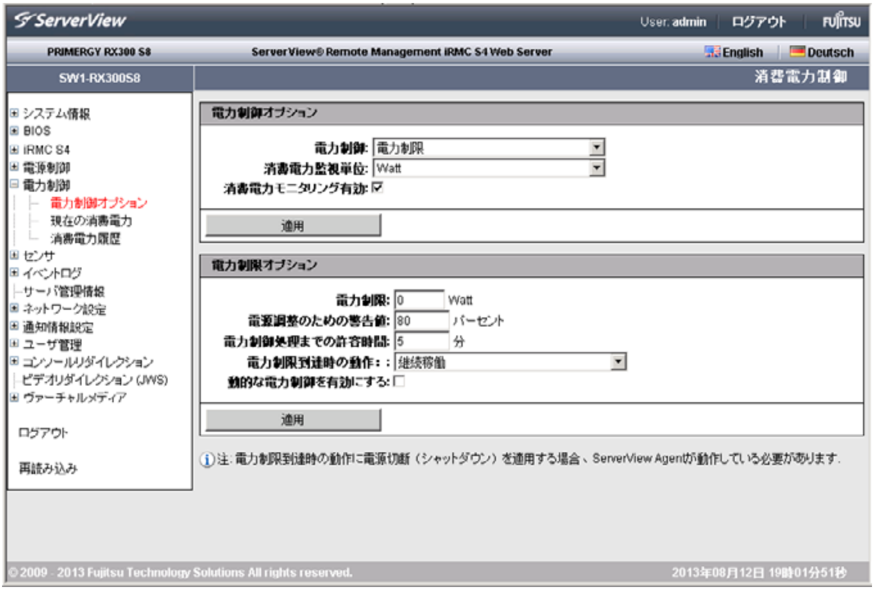


図 108: 「消費電力制御」ページ - 電力制限オプション

電力制限

最大消費電力（単位：Watt）。

これに達すると、「*電力制限到達時の動作*」で定義した動作が実行されます。しきい値を超過すると、iRMC S4 SEL に警告メッセージが書き込まれます（「CPU Throttlink activated by Power Capping」）。

電源調整のための警告値

iRMC S4 は、「*電力制限*」で指定された最大消費電力のパーセンテージとして指定されるこの値に合わせて、消費電力を調整しようとします。

電力制御処理までの許容時間

*電力制限*を超過してからシステムが待機する時間（分）。その後、「*電力制限到達時の動作*」で指定された動作が実行されます。

電力制限到達時の動作

*電力制限*が「*電力制限の据置期間*」で指定した期間を経過したときに実行する動作。

継続稼働

動作は行われません。

電源切断（シャットダウン）

システムを「適切に」シャットダウンし、電源を切断します。

i このオプションは、ServerView エージェントがインストールされていて、かつ、iRMC S4 にサインオンして「接続中」の場合のみサポートされます。

電源切断

オペレーティングシステムの状態にかかわらず、サーバの電源を切断します。

動的な電力制御を有効にする

電力制限を動的に制御します。このオプションが有効な場合、「*電力制限*」を超過すると、iRMC S4 はサーバの消費電力を下げます。iRMC S4 は、「*Target for Power Regulation*」で指定されたレベルに合わせて消費電力を調整します。

7.9.2 現在のシステム消費電力 - 消費電力の表示

> **i** このビューは、iRMC S4 が搭載される一部の PRIMERGY サーバではサポートされていません。

「*現在のシステム消費電力*」ページには、システムのコンポーネントおよびシステム全体の現在の消費電力が表示されます。

図 109: 「現在のシステム消費電力」ページ

7.9.3 消費電力モニタリング履歴 - 消費電力の表示

「*消費電力モニタリング履歴*」ページには、PRIMERGY サーバの消費電力のグラフが表示されます。

> **i** このページは、iRMC S4 が搭載される一部の PRIMERGY サーバでサポートされていません。

図 110: 「消費電力モニタリング履歴」ページ

現在の全体消費電力

このオプションは、一部の PRIMERGY サーバではサポートされていません。

「*現在の全体消費電力*」では、現状設定された間隔で計測したサーバの消費電力の情報が表示されています。現在の電力、最小電力、ピーク電力および平均電力が表示されます。

グラフ形式で、サーバの可能な最大消費電力量と現在の消費電力量を比較して表示しています。

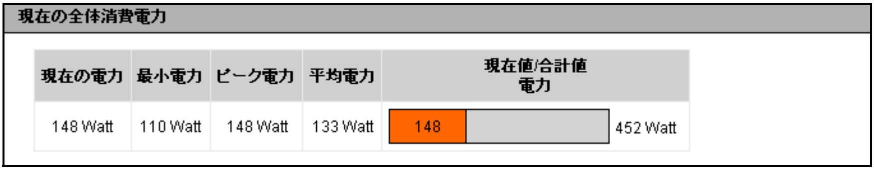


図 111: 「消費電力モニタリング履歴」ページ - 現在の全体消費電力

消費電力モニタリング履歴表示オプション

消費電力モニタリング履歴表示オプションでは、消費電力を表示するパラメータを設定することができます。

図 112: 「消費電力モニタリング履歴」ページ - 消費電力モニタリング履歴表示オプション

消費電力監視単位

電力単位：

– Watt

– *BTU/h*（BTU/ 時（British Thermal Unit/ 時、1 BTU/ 時は 0.293 ワットに相当します。）

消費電力表示期間

消費電力のグラフの表示期間。

以下の間隔を選択できます。

1 時間

デフォルト。
最新の 1 時間を計測します（60 の値）。1 分間毎に計測が行われますので、最新の 1 時間の計測値を表示します。

12 時間

最新の 12 時間を計測します。5 分間隔で計測され、表示されます（5 番目毎の計測、全部で 144 の値）。

1 日

最新の ２４ 時間を計測します。10 分間隔で計測し、表示します（10 番目毎の計測、全部で 144 の値）。

1 週間

最新の 1 週間を計測します。1 時間間隔で計測し、表示します（60 番目毎の計測､、全部で 168 の値）。

2 週間

最新の 1 週間を計測します。およそ 4 時間間隔で計測し、表示します（120 番目毎の計測、全部で 168 の値）。

1ヶ月

最新の 6 ヶ月を計測します。およそ 1 日間隔で計測し、表示します（240 番目毎の 計測、全部で 180 の値）。

1 年間

最新の 12 ヶ月を計測します。2 日間隔で計測され、表示されます（2880 番目毎の 計測、全部で 180 の値）。

5 年間

最新の 5 年間を計測します。2 日間隔で計測され、表示されます（2880 番目毎の 計測、全部で 180 の値）。

消費電力モニタリング有効

電力監視を実行するかどうかを指定します。

> **i** 電力監視はデフォルトでは有効です。

> **i** この設定は、消費電力のログの記録をサポートしている PRIMERGY サーバのみに適用できます。

► 「*適用*」をクリックすると設定が有効になります。

► 「*履歴の消去*」ボタンをクリックして、表示されているデータを消去します。

消費電力グラフ表示

「*消費電力グラフ表示*」には、グラフ形式で管理対象サーバの消費電力量が表示されます（「*消費電力履歴オプション*」を使用します）。実際の消費電力と「消費電力グラフ表示」に表示される消費電力の差が、約 20% になることがあります。

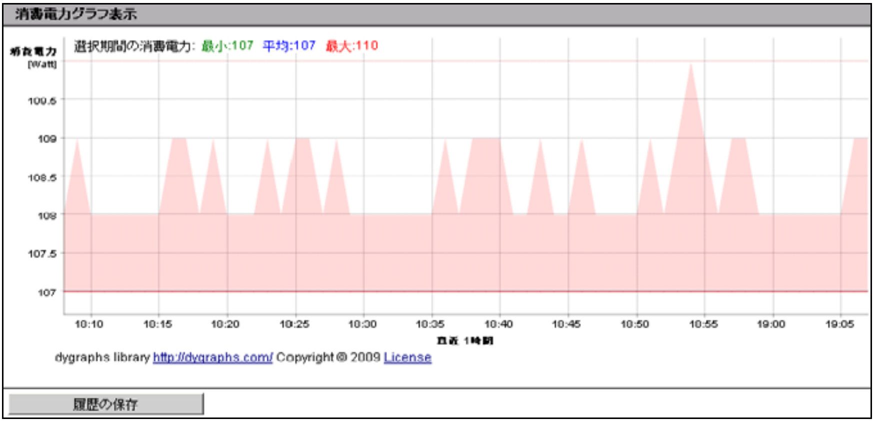


図 113: 「消費電力モニタリング履歴」ページ - 消費電力グラフ表示

7.10 センサ - センサの状態確認

「センサ」エントリには、管理対象サーバのセンサのステータスをチェックするページがあります。

– 204 ページ の「ファン - ファン状態確認」
– 206 ページ の「温度 - サーバコンポーネントの温度のレポート」
– 208 ページ の「電圧 - 電圧センサ情報のレポート」
– 209 ページ の「電源装置個別情報 - 電源ユニットの状態確認」
– 211 ページ の「コンポーネント - サーバコンポーネントの状態確認」

状態チェックが容易にできるように、センサの状態は現在値を表示するだけでなく、カラーコードと状態アイコンも使用しています。

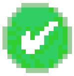
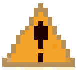
黒色 （フォントカラー） 	測定値は稼動時の正常な値の範囲内にあります。
オレンジ色 （フォントカラー） 	測定値は警告のしきい値を超えています。 システムの稼動状態は、まだ危険な状態ではありません。
赤色 （フォントカラー） 	測定値は致命的しきい値を超えています。 システムの稼動状態は、危険な状態にある可能性があり、データ喪失の危険があります。

表 7: センサの状態

7.10.1 ファン - ファン状態確認

「ファン」ページには、ファンおよびそれらの状態に関する情報が表示されます。

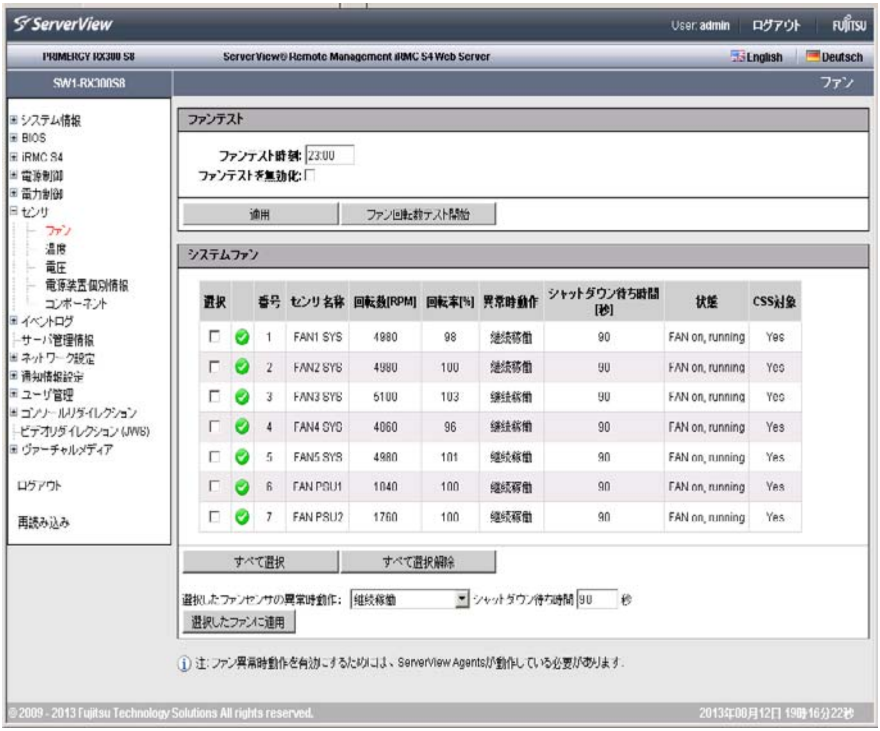


図 114: 「ファン」ページ

ファンテスト - ファンのテスト

「*ファンテスト*」グループでは、ファンのテストを自動的に開始する時刻を設定したり、手動で開始したりできます。

> **i** 「*ファンテスト*」では、現在必要な速度に近い速度でファンテストを実行します。そのため、ファンテストは聴覚的には目立ちません。

ファンテスト時刻

ファンテストが自動的に開始される時刻を入力します。

ファンテストを無効化

このオプションを選択すると、ファンテストが行われなくなります。

- 「*適用*」をクリックすると設定が有効になります。
- 「*ファン回転数テスト開始*」をクリックして、ファンのテストを開始します。

システムファン - ファンが故障した場合のサーバ動作の設定

「*システムファン*」グループを使って、ファンの状態に関する情報を確認することができます。オプションおよびボタンを個々のファンまたはすべてのファンに対して有効にすることができます。また、ファンが故障した場合、何秒後にサーバをシャットダウンするか否かを設定することができます。

すべて選択
すべてのファンを選択します。

すべて選択解除
すべての選択を解除します。

- 故障時に特別な処置を行うファンを選択します。
- ワークエリアの下方のリストを使って、故障発生時の動作を定義します。
  - 「*継続稼働*」を選択すると、選択されたすべてのファンが故障してもサーバはシャットダウンされません。
  - 「*シャットダウン & 電源断*」を選択すると、選択されたファンが故障した場合、サーバはシャットダウンされ、電源が切断されます。このオプションを選択する場合、リストの右のフィールドで、ファンの故障からシャットダウンまでの時間（シャットダウン待ち時間）を設定します。

    i 冗長ファンの場合、2 つ以上のファンが故障し、「*シャットダウン & 電源断*」がこれらのファンに設定されている場合のみ、シャットダウンが実行されます。

- 「*選択したファンに適用*」をクリックして、選択したファンへの設定を有効にしてください。

7.10.2 温度 - サーバコンポーネントの温度のレポート

「*温度*」ページには、CPU、メモリモジュールおよび周囲の温度など、温度センサが計測したサーバのコンポーネントの温度情報が表示されます。

図 115: 「温度」ページ

オプションおよびボタンを、個々の温度センサあるいはすべての温度センサに対して有効にすることができます。また、選択されたセンサが危険温度に達した場合、サーバをシャットダウンするかどうかの設定を行うこともできます。

すべて選択

すべての温度センサを選択します。

すべて選択解除

すべての選択を解除します。

- ▶ 危険温度に達した場合の動作を定義するセンサを選択します。
- ▶ ワークエリアの下方のリストを使って、危険温度到達時の動作を定義します。
  - –「*継続稼働*」を選択すると、選択されたセンサが危険温度に達してもサーバはシャットダウンされません。
  - –「*シャットダウン & 電源断*」を選択すると、選択されたセンサが危険温度に達した場合、サーバはシャットダウンされ、電源が切断されます。
- ▶「*選択したセンサに適用*」ボタンをクリックして、選択した温度センサへの設定を有効にしてください。

7.10.3 電圧 - 電圧センサ情報のレポート

「*電圧*」ページには、サーバのコンポーネントに割り当てられた電圧センサの状態に関する情報が表示されます。

図 116: 「電圧」ページ

7.10.4 電源装置個別情報 - 電源ユニットの状態確認

「*電源装置個別情報*」ページには、電源ユニットに関する情報が表示されます。一部のタイプのサーバでは、「*電源装置個別情報*」ページで電源ユニットの冗長設定を行うこともできます。

図 117: 「電源装置個別情報」ページ

iRMC S4 でのサポート
電源冗長構成

> i この機能は、2 台以上の PSU を搭載するシステムでのみ設定できます。

「*電源冗長構成*」グループでは、管理対象サーバに冗長モードを設定できます。実際に使用できるオプションはサーバの機能によって異なります。

PSU Redundancy 1 + 1 予備 PSU
合計 2 台の PSU の場合に、1 台の PSU が故障してもシステムの稼働が保証されます。

PSU Redundancy 2 + 1 予 備 PSU
合計 3 台の PSU の場合に、1 台の PSU が故障してもシステムの稼働が保証されます。

PSU Redundancy 3 + 1 予備 PSU
合計 4 台の PSU の場合に、1 台の PSU が故障してもシステムの稼働が保証されます。

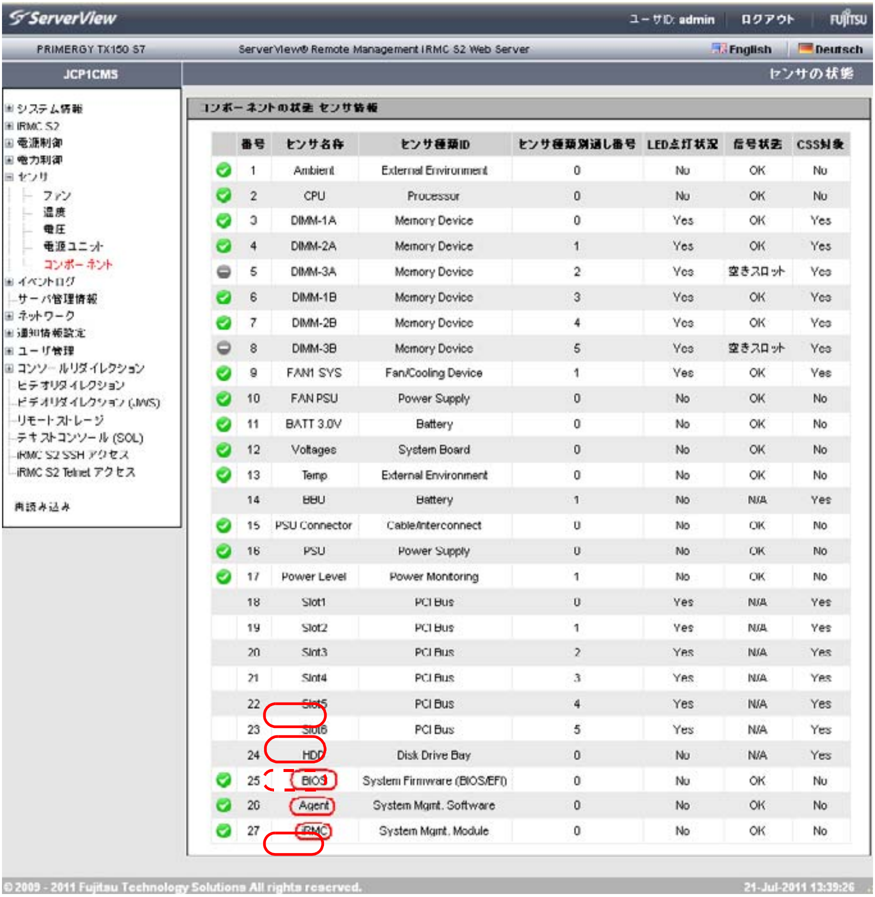
AC Redundancy 2 + 2 (2AC 電源)
4 台の PSU のうち 2 台がそれぞれ別個の AC ソースに接続されます。これにより、電力線や 1 台の PSU が故障しても、システムは稼働し続けることができます。

AC Redundancy 1 + 1 (2AC 電源)
（合計 2 台の PSU の）各 PSU が別個の AC ソースに接続されます。これにより、電力線や 1 台の PSU が故障しても、システムは稼働し続けることができます。

7.10.5 コンポーネント - サーバコンポーネントの状態確認

「*コンポーネント*」ページには、サーバのコンポーネントの状態に関する情報が表示されます。「*CSS 対象*」列には、各コンポーネントの CSS（**C**ustomer **S**elf **S**ervice）機能のサポートの有無が示されます。

サーバシャーシを開くと、「*センサの状態*」ページの対応する「*Identify*」ボタンをクリックして、LED を搭載するコンポーネントを容易に識別できます。



番号	センサ名称	センサ種類ID	センサ種類別通し番号	LED点灯状況	信号状態	CSS対象
1	Ambient	External Environment	0	No	OK	No
2	CPU	Processor	0	No	OK	No
3	DIMM-1A	Memory Device	0	Yes	OK	Yes
4	DIMM-2A	Memory Device	1	Yes	OK	Yes
5	DIMM-3A	Memory Device	2	Yes	空きスロット	Yes
6	DIMM-1B	Memory Device	3	Yes	OK	Yes
7	DIMM-2B	Memory Device	4	Yes	OK	Yes
8	DIMM-3B	Memory Device	5	Yes	空きスロット	Yes
9	FAN1 SYS	Fan/Cooling Device	1	Yes	OK	Yes
10	FAN PSU	Power Supply	0	No	OK	No
11	BATT 3.0V	Battery	0	No	OK	No
12	Voltages	System Board	0	No	OK	No
13	Temp	External Environment	0	No	OK	No
14	BBU	Battery	1	No	N/A	Yes
15	PSU Connector	Cable/Interconnect	0	No	OK	No
16	PSU	Power Supply	0	No	OK	No
17	Power Level	Power Monitoring	1	No	OK	No
18	Slot1	PCI Bus	0	Yes	N/A	Yes
19	Slot2	PCI Bus	1	Yes	N/A	Yes
20	Slot3	PCI Bus	2	Yes	N/A	Yes
21	Slot4	PCI Bus	3	Yes	N/A	Yes
22	Slot5	PCI Bus	4	Yes	N/A	Yes
23	Slot6	PCI Bus	5	Yes	N/A	Yes
24	HDD	Disk Drive Bay	0	No	N/A	Yes
25	BIOS	System Firmware (BIOS/EFI)	0	No	OK	No
26	Agent	System Mgmt. Software	0	No	OK	No
27	iRMC	System Mgmt. Module	0	No	OK	No

図 118: 「コンポーネント」ページ

識別

関連するサーバコンポーネントの LED が点灯します。LED のラベルは「*Identify Off*」になります。ステータスアイコンの代わりに緑色の LED 記号が「*センサの状態*」ページの一番左の列に表示されます。

> サーバコンポーネントに LED がない場合、「*Identify*」ボタンがグレー表示されラベルが「*No LED*」になります。

LED Off

関連するサーバコンポーネントの LED が消灯します。LED のラベルは「*Identify*」になります。「*センサの状態*」ページの一番左の列の緑色の LED 記号が表示されなくなり、再びステータス記号が表示されます。

「センサ名称」のエントリの「iRMC」、「Agent」、「BIOS」、「VIOM」

「*センサ名称*」のエントリの「iRMC」、「Agent」、「BIOS」、「VIOM」は、iRMC S4、エージェント、BIOS または VIOM がエラーを検出したことを示します。これは、iRMC S4、エージェント、BIOS、VIOM 自体が故障していることを意味するものではありません。

Designation「HDD」および「HDD<n>」を含むエントリ、エージェントレス HDD 監視（「アウトオブバンド」HDD 監視）

Designation「HDD」または「HDD<n>」（n = 1、2、...）を含むエントリは、ハードディスクドライブ（HDD）のステータスを示します：

– HDD コンポーネントステータスは、ServerView RAID がインストールされている場合のみ表示されます。

– *Designation*「HDD」を含むエントリは、個々の HDD のステータスをまとめることにより、サーバの HDD 全体のステータスを示します。

– サーバの HDD 全体のステータスは、ServerView エージェントと ServerView RAID Manager によって、読み取られて iRMC S4 に報告されます。

– *Designation*「HDD<n>」（n = 1、2、...）を含むエントリは、個々の HDD のステータスを示します。

> **なお、次の点に注意してください。**
>
> – iRMC S4 がこの機能をサポートするのは、バックプレーンがこの機能をサポートする場合のみです。
>
> – この機能は、OOB_RAID がアクティブな場合は非アクティブです。

– この機能は、管理対象の PRIMERGY サーバが「エージェントレス HDD 監視」機能（「帯域外 HDD 監視」としても知られています）をサポートする場合のみサポートされます。

これらの要件が満たされる場合、各 HDD の HDD<n> ステータスが iRMC S4 に直接報告されます。ServerView エージェントは使用されません。

	59	HDD1	Disk Drive Bay	1	No	OK	Yes
	60	HDD2	Disk Drive Bay	2	No	Prefail	Yes
	61	HDD3	Disk Drive Bay	3	No	Failed	Yes
	62	HDD4	Disk Drive Bay	4	No	OK	Yes

図 119: 個々の HDD のステータス表示

– サーバの HDD 全体のステータスは、ServerView エージェントと ServerView RAID Manager によって、読み取られて iRMC S4 に報告されます。

そのため、「*コンポーネントの状態 センサ情報*」表に表示される厳密なエントリは、サーバの状態と、サーバが「エージェントレス HDD 監視」機能をサポートするかどうかによって異なります：

– 「*センサ名*」のエントリの「HDD」には、ServerView エージェントと ServerView RAID Manager がインストールされていて、管理対象サーバで実行されている場合のみ、「*信号状態*」カラムにステータス
が表示されます。そうでない場合は、「*信号状態*」カラムに代わりに「N/A」（該当なし）と表示されます。

– HDD コンポーネントステータスは表示されません。

– 「*Prefail*」ステータスは、すべての HDD でサポートされるわけではありません。

– 「*センサ名* 」のエントリの「HDD<n>（n = 1、2、...）」は、管理対象サーバが「エージェントレス HDD 監視」機能をサポートする場合のみ表示されます。

7.11 イベントログ

ナビゲーション領域の「*イベントログ*」エントリには、IPMI イベントログ（システムイベントログ（SEL））と iRMC S4 の内部イベントログの表示および設定を行うページへのリンクが含まれます。

– 215 ページ の「システムイベントログ内容 - SEL および SEL エントリに関する情報の表示」

  内部イベントログには、監査イベントに関する情報（ログオンイベント、AVR 接続イベントなど）やその他の情報（IPv6 関連の情報および LDAP ユーザ名など）を提供するエントリが含まれます。

– 218 ページ の「イベントログ情報 - 内部イベントログと関連するエントリに関する情報の表示」

  IPMI SEL には、オペレーティングシステムのブート / シャットダウン、ファンの故障、iRMC S4 ファームウェアのフラッシュなどのイベントに関する情報を提供するエントリが含まれます。

– 221 ページ の「システムイベントログ設定 - IPMI SEL と内部イベントログの設定」

色付きのアイコンが、それぞれのイベントまたはエラーカテゴリに割り当てられています。

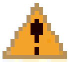
	Critical
	重度
	軽度
	情報
	顧客自己保守（CSS）イベント

表 8: システムイベントログ / 内部イベントログの内容 - エラーカテゴリ

7.11.1 システムイベントログ内容 - SEL および SEL エントリに関する情報の表示

「*システムイベントログ内容*」ページには、IPMI SEL に関する情報と SEL エントリが表示されます。IPMI SEL には、オペレーティングシステムのブート / シャットダウン、ファンの故障、iRMC S4 ファームウェアのフラッシュなどのイベントに関する情報を提供するエントリが含まれます。

「*CSS Event*」列には、各イベントについて、イベントが CSS（**C**ustomer **S**elf **S**ervice）コンポーネントによってトリガされたかどうかを示します。

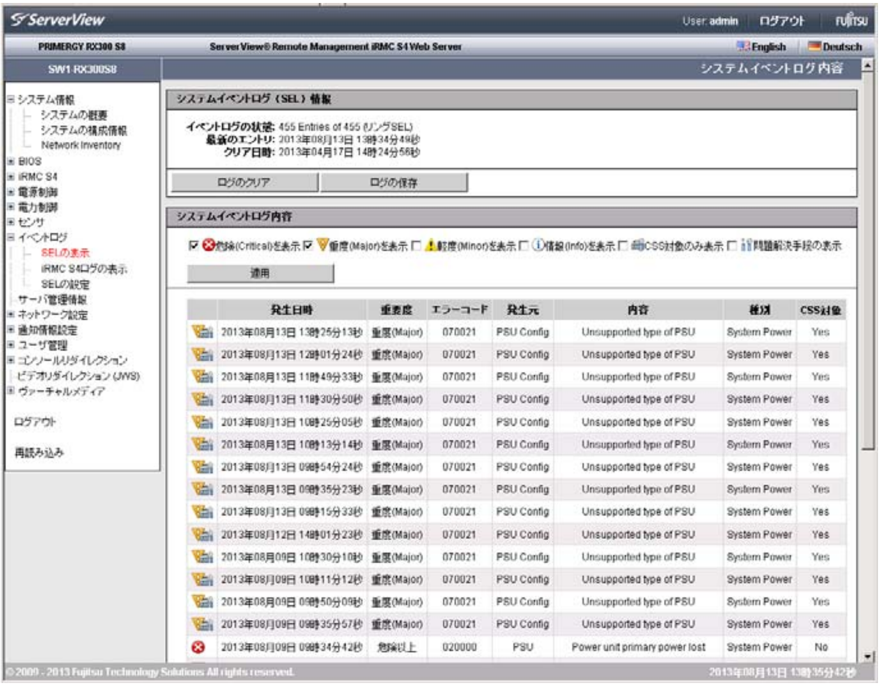


図 120: 「システムイベントログ内容」ページ

システムイベントログ (SEL) 情報

「*システムイベントログ (SEL) 情報*」グループには、IPMI SEL 内のエントリ数の情報が表示されます。最後のエントリがいつ追加または削除されたかも表示します。

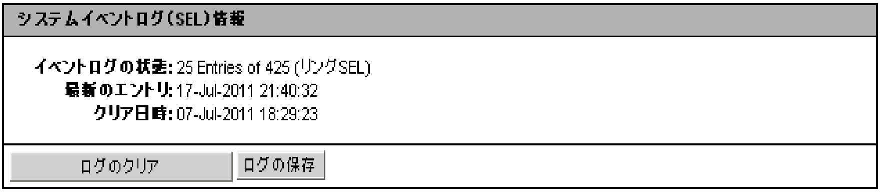


図 121: 「システムイベントログ内容」ページ - システムイベントログ (SEL) 情報

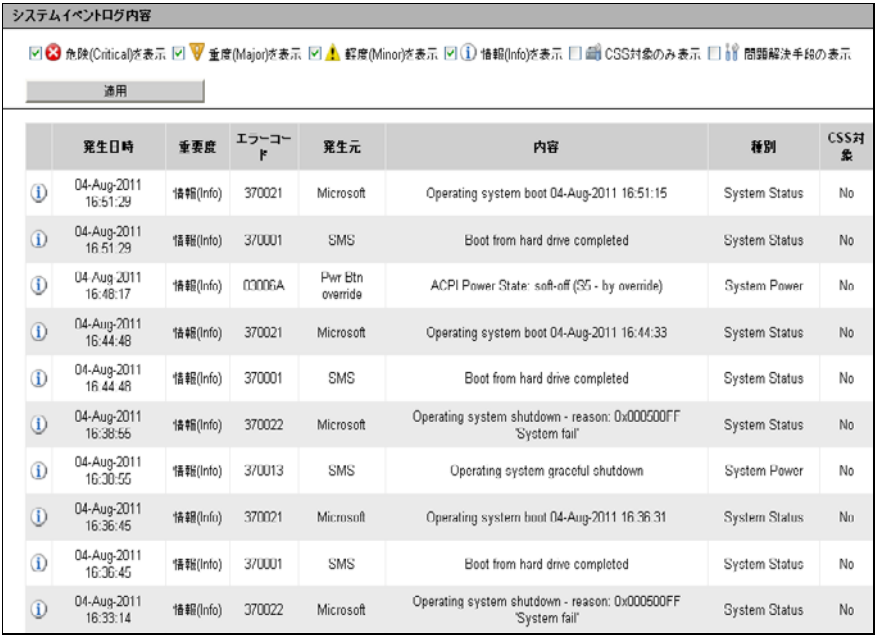
ログのクリア
: 「*ログのクリア*」ボタンをクリックすると、IPMI SEL 内のすべてのエントリを消去することが できます。

ログの保存
: 「*ログの保存*」ボタンをクリックした後、IPMI SEL のエントリを含む *iRMC S4 EventLog.sel* ファイルをダウンロードできます。

システムイベントログ内容

「*システムイベントログ内容*」グループには、重要度によってフィルタリングされた SEL エントリが表示されます。

> **i** 「*システムイベントログ内容*」グループで、現在のセッション中にフィルタ条件を変更できます。ただし、ここで行う設定は次のログアウトまでしか有効でありません。その後は、デフォルト設定がまた適用されます。



システムイベントログ内容

危険(Critical)を表示 重度(Major)を表示 軽度(Minor)を表示 情報(Info)を表示 CSS対象のみ表示 問題解決手段の表示

適用

	発生日時	重要度	エラーコード	発生元	内容	種別	CSS対象
	04-Aug-2011 16:51:29	情報(Info)	370021	Microsoft	Operating system boot 04-Aug-2011 16:51:15	System Status	No
	04-Aug-2011 16:51:29	情報(Info)	370001	SMS	Boot from hard drive completed	System Status	No
	04-Aug-2011 16:48:17	情報(Info)	C0006A	Pwr Btn override	ACPI Power State: soft-off (S5 - by override)	System Power	No
	04-Aug-2011 16:44:48	情報(Info)	370021	Microsoft	Operating system boot 04-Aug-2011 16:44:33	System Status	No
	04-Aug-2011 16:44:48	情報(Info)	370001	SMS	Boot from hard drive completed	System Status	No
	04-Aug-2011 16:38:55	情報(Info)	370022	Microsoft	Operating system shutdown - reason: 0x000500FF 'System fail'	System Status	No
	04-Aug-2011 16:38:55	情報(Info)	370013	SMS	Operating system graceful shutdown	System Power	No
	04-Aug-2011 16:36:45	情報(Info)	370021	Microsoft	Operating system boot 04-Aug-2011 16:36:31	System Status	No
	04-Aug-2011 16:36:45	情報(Info)	370001	SMS	Boot from hard drive completed	System Status	No
	04-Aug-2011 16:33:14	情報(Info)	370022	Microsoft	Operating system shutdown - reason: 0x000500FF 'System fail'	System Status	No

図 122: 「システムイベントログ内容」ページ - システムイベントログ内容

危険(Critical)を表示、重度(Major)を表示、軽度(Minor)を表示、情報(Info)を表示、CSS 対象の未表示

必要に応じて、このデフォルト値以外の 1 つ以上の重大度レベルを選択することもできます。

問題解決手段の表示

このオプションを選択すると、重大度レベル「*Critical*」または「*Major*」の各 SEL エントリについて、推奨される問題解決手段が表示されます。

▶ 「*適用*」をクリックして、現在のセッション中に設定を有効にします。

7.11.2 イベントログ情報 - 内部イベントログと関連するエントリに関する情報の表示

「*iRMC S4 イベントログ情報*」ページには、内部イベントログに関する情報と、関連するエントリが表示されます。内部イベントログには、監査イベント（ログオンイベント、AVR 接続イベントなど）およびその他の情報（IPv6 関連の情報および LDAP ユーザ名など）が含まれます。

図 123: 「iRMC S4 イベントログ情報」ページ

iRMC S4 イベントログ情報

「*iRMC S4 イベントログ情報*」グループには、内部イベントログ内のエントリ数の情報が表示されます。最後のエントリがいつ追加または削除されたかも表示します。

図 124: 「イベントログ情報」ページ - iRMC S4 イベントログ情報

イベントログのクリア
: 「*イベントログのクリア*」をクリックすると、内部イベントログ内のすべてのエントリを消去することが できます。

イベントログの保存
: 「*イベントログの保存*」ボタンをクリックした後、iRMC S4 で、内部イベントログのエントリを含むファイル *iRMC S4_InternalEventLog.sel* をダウンロードできます。

iRMC S4 イベントログ内容

「*iRMC S4 イベントログ内容*」グループには、重要度によってフィルタリングされた内部イベントログエントリが表示されます。

> **i** 「*iRMC S4 イベントログ内容*」グループで、現在のセッション中にフィルタ条件を変更できます。ただし、ここで行う設定は次のログアウトまでしか有効でありません。その後は、デフォルト設定がまた適用されます。

	発生日時	重要度	エラーコード	内容	種別
	2013年08月13日 13時45分36秒	情報(Info)	2300B1	iRMC S4 Browser http connection user 'admin' login from 172.17.167.181	Security
	2013年08月13日 13時25分30秒	情報(Info)	2300B1	iRMC S4 Browser http connection user 'admin' login from 172.17.167.181	Security
	2013年08月13日 12時32分14秒	情報(Info)	2300B1	iRMC S4 Browser http connection user 'admin' login from 172.17.167.181	Security
	2013年08月13日 12時14分40秒	情報(Info)	2300B1	iRMC S4 Browser http connection user 'admin' login from 172.25.101.191	Security
	2013年08月12日 19時29分02秒	情報(Info)	2300B2	iRMC S4 Browser http connection user 'admin' logout from 172.17.167.181	Security
	2013年08月12日 17時26分27秒	情報(Info)	2300B1	iRMC S4 Browser http connection user 'admin' login from 172.17.167.181	Security
	2013年08月12日 17時26分18秒	情報(Info)	2300E4	iRMC S4 Browser http connection user 'admin' auto-logout from 172.17.167.181	Security
	2013年08月12日 17時26分18秒	情報(Info)	2300E4	iRMC S4 Browser http connection user 'admin' auto-logout from 172.17.167.181	Security
	2013年08月12日 17時26分14秒	情報(Info)	2300B0	iRMC S4 Browser AVR connection user 'admin' AVR Session finished from 172.17.167.181	Security

図 125: 「イベントログ情報」ページ - iRMC S4 イベントログ内容

危険（Critical）を表示、*重度（Major）を表示*、*軽度（Minor）を表示*、*情報（Info）を表示*

必要に応じて、このデフォルト値以外の 1 つ以上の重大度レベルを選択することもできます。

► 「*適用*」をクリックして、現在のセッション中に設定を有効にします。

7.11.3 システムイベントログ設定 - IPMI SEL と内部イベントログの設定

「*システムイベントログ設定*」ページでは、IPMI SEL（システムイベントログ）および内部イベントログを設定できます。

各イベントログについて以下を設定できます。

– デフォルトで「*システムイベントログ内容*」ページ（215 ページを参照）と「*iRMC S4 イベントログ内容*」ページ（218 ページを参照）にそれぞれ表示されるエントリ

– IPMI SEL と内部イベントログを、リングバッファまたはリニアバッファとして構成するかどうか

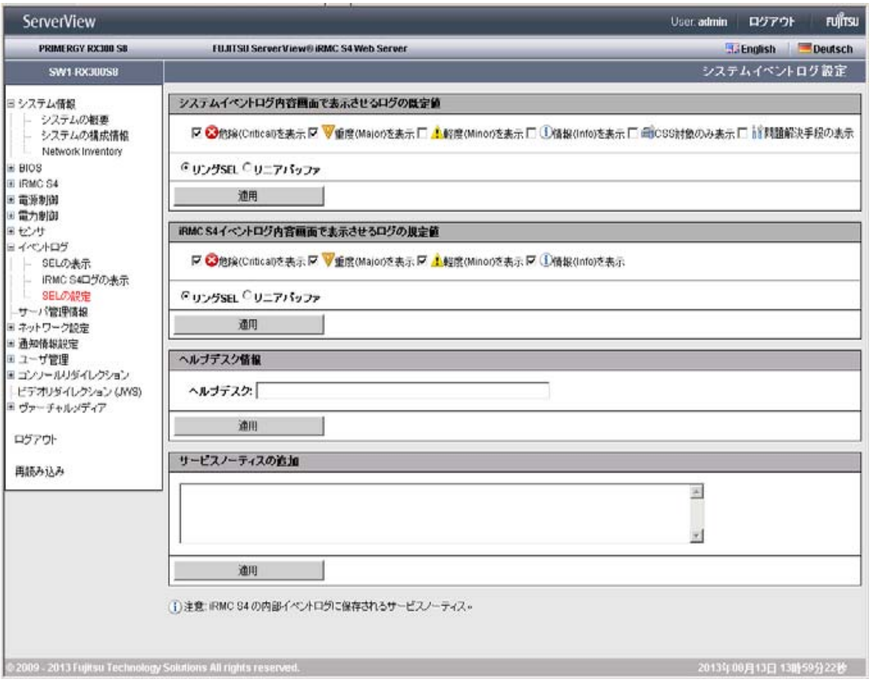


図 126: 「システムイベントログ設定」ページ

IPMI イベントログ設定

LCD パネルに表示させるシステムイベントログの規定値

> **i** ServerView Local Service Display モジュールが管理対象 PRIMERGY サーバに取り付けられている場合、エラー重大度を選択して ServerView Local Service Display に SEL を表示することもできます。（この選択は、「*システムイベントログ内容*」ページに表示される SEL エントリに行った選択とは関係ありません。）

危険（Critical）を表示、重度（Major）を表示、軽度（Minor）を表示、情報（Info）を表示、CSS 対象の未表示

イベントログエントリを ServerView Local Service Display にデフォルトで表示する、1 つ以上の重大度レベルを選択します。

システムイベントログ内容画面で表示させるログの既定値

危険（Critical）を表示、重度（Major）を表示、軽度（Minor）を表示、情報（Info）を表示、CSS 対象の未表示

イベントログエントリを「*システムイベントログ内容*」ページ（215 ページを参照）にデフォルトで表示する、1 つ以上の重大度レベルを選択します。

問題解決手段の表示

このオプションを選択すると、重大度レベル「*Critical*」、「*Major*」、「*Minor*」の各 SEL エントリについて、エントリの理由、および推奨される問題解決手段が表示されます。

リング SEL

イベントログはリングバッファとして構成されます。

リニアバッファ

イベントログはリニアバッファとして構成されます。

> **i** リニアイベントログが完全にフルになると、それ以上エントリを追加できなくなります。

► 「*適用*」をクリックすると設定が有効になります。

iRMC S4 イベントログ内容画面で表示させるログの規定値

危険（Critical）を表示、重度（Major）を表示、軽度（Minor）を表示、情報（Info）を表示

イベントログエントリを「*システムイベントログ内容*」ページ（218 ページを参照）にデフォルトで表示する、1 つ以上の重大度レベルを選択します。

リング SEL

イベントログはリングバッファとして構成されます。

リニアバッファ

イベントログはリニアバッファとして構成されます。

> i リニアイベントログが完全にフルになると、それ以上エントリを追加できなくなります。

► 「*適用*」をクリックすると設定が有効になります。

ヘルプデスク情報

図 127: 「システムイベントログ設定」ページ - ヘルプデスク情報

ヘルプデスク

ヘルプデスクの表示に使用する文字列

► 「*適用*」をクリックすると設定が有効になります。

サービスノーティスの追加

「*サービスノーティスの追加*」グループのテキストフィールドに、iRMC S4 の内部イベントログに格納されるサービス注記を入力できます。

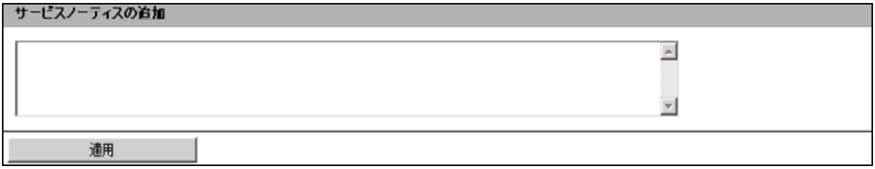


図 128: 「システムイベントログ設定」ページ - サービスノーティスの追加

► 「*適用*」をクリックすると設定が有効になります。

7.12 サーバ管理情報 - サーバ設定の編集

「*サーバ管理情報*」ページを使用して、サーバに以下の設定を行うことができます。

– サーバの ASR&R（Automatic Server Reconfiguration and Restart）設定（225 ページを参照）

– ウォッチドッグ設定（226 ページを参照）

– HP System Insight Manager（HP SIM）との連携（228 ページを参照）

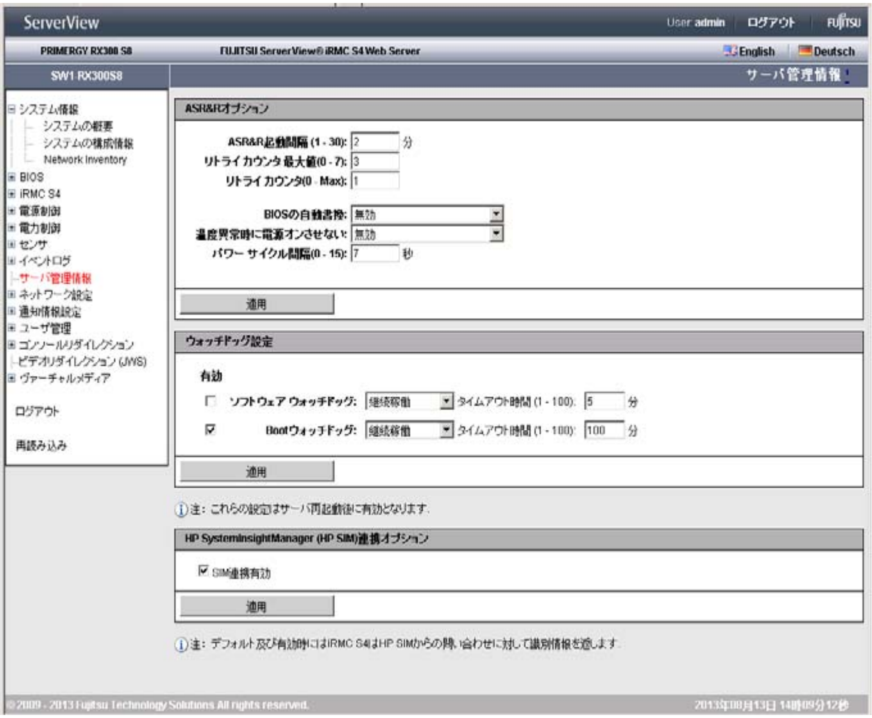


図 129: 「サーバ管理情報」ページ

ASR&R オプション - ASR&R 設定

「*ASR&R オプション*」グループを使用して、サーバの ASR&R（Automatic Server Reconfiguration and Restart）設定を行うことができます。

> i 「*ASR&R オプション*」グループで行う設定は、管理対象サーバの次回の起動時から有効になります。

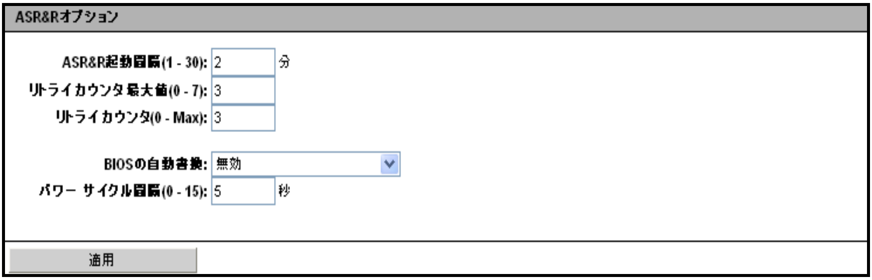


図 130: 「サーバ管理情報」ページ - ASR&R オプション

ASR&R 起動間隔（1 - 30）
: サーバが再起動する前の遅延時間（分）（1 ～ 30 分）

リトライカウンタ最大値（0 - 7 ）
: 重大なエラー発生後にサーバに許可する最大リスタート回数（最大 7 回）

リトライカウンタ（0 - Max）
: 重大なエラー発生後にサーバが試行するリアルタイムスタート試行回数（最大値は「*リトライカウンタ最大値*」に設定された値）

BIOS の自動書換
: BIOS リカバリフラッシュビットを有効 / 無効にします。

  – *有効*
    次回のシステム起動時に、BIOS を自動で書き換えます。

  – *無効*
    次回のシステム起動時に、BIOS を自動で書き換えません。

> **i** この値を「*有効*」に設定すると、ファームウェアがアップデートされるまで、オペレーティングシステムは起動しません。
> BIOS リカバリフラッシュが、次回のシステム起動時に DOS フロッピーから（あるいは DOS フロッピーイメージから）自動で実行されます。
>
> BIOS リカバリフラッシュが成功してから、BIOS リカバリフラッシュビットを「*無効*」に再設定してください。

温度異常時に電源オンさせない
有効な場合、クリティカルな温度が発生した場合に、サーバの電源が入らないようにできます。

パワーサイクル間隔（0 - 15）
電源オフから電源オンまでの間の間隔（秒）を設定します。

► 「*適用*」をクリックすると設定が保存します。

設定が保存され、適切な条件件が満たされると動作が実行されます。

ウォッチドッグ設定 - ソフトウェアウォッチドッグおよび Boot ウォッチドッグの設定

「*ウォッチドッグ設定*」グループを使用して、ソフトウェアウォッチドッグおよび Boot ウォッチドッグを設定できます。

> **i** 「*ASR&R オプション*」グループで行う設定は、管理対象サーバの次回の起動時から有効になります。

図 131: 「サーバ管理情報」ページ - ウォッチドッグオプション

ソフトウェアウォッチドッグ

ServerView エージェントを使用して、システムの動作を監視します。ソフトウェアウォッチドッグは、ServerView エージェントとオペレーティングシステムが完全に初期化されたときに有効になります。
ServerView エージェントは、事前に定義された間隔で iRMC S4 にアクセスします。

ServerView エージェントからのメッセージが届かない場合は、システムが正常に機能しなくなったと考えられます。
このようになった場合に実行するアクションを指定できます。

Boot **ウォッチドッグ**は、システムの起動と ServerView エージェントが使用可能な時間との間のフェーズを監視します。
ServerView エージェントが指定された時間内にサーバの iRMC S4 への接続を確立しない場合、起動プロセスが正常に実行されなかったと考えられます。
このようになった場合に実行するアクションを指定できます。

次の手順に従います。

► 「*ソフトウェアウォッチドッグ*」および「*Boot ウォッチドッグ*」について、「有効」の下のチェックボックスにチェックするかチェックを外します。

► これらのチェックボックスにチェックした場合、「*ソフトウェアウォッチドッグ*」および「*Boot ウォッチドッグ*」の後ろの以下の設定ができます。

継続稼働
: ウォッチドッグが時間切れしても、何の動作も行われず、サーバは稼動を続けます。イベントログに記録されます。

リセット
: サーバ管理ソフトウェアが、システムリセットを行います。

パワーサイクル
: サーバの電源が切断され、再び直ちに電源投入されます。

► 必要に応じて、「*タイムアウト時間(1 - 100)*」の後にこの動作を実行するまでの待機時間(分)を入力します。

> **i** Boot ウォッチドッグは、システムが起動するまで待機します。そのため、「*タイムアウト時間(1- 100)*」には、十分な時間を設定してください。

► 「*適用*」ボタンをクリックします。

設定が保存され、適切な条件が満たされると動作が実行されます。

HP SystemInsight Manager（HP SIM）連携オプション - HP SIM 連携の設定

「*HP SystemInsight Manager （HP SIM) 連携オプション*」グループを使用して、iRMC S4 デバイスが、HP SystemInsight Manager から送信される非公式の XML 問い合わせに対する応答として、ある識別情報を返すように設定することができます。

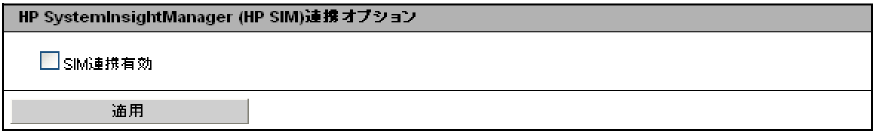


図 132: 「サーバ管理情報」ページー HP SystemInsight Manager（HP SIM）連携オプション

次の手順に従います。

- ► HP SIM との連携を無効あるいは有効にするために、「*SIM 連携有効*」チェックボックスをオンまたはオフにします。
- ► 「*適用*」をクリックすると設定が有効になります。

7.13 ネットワーク設定 - LAN パラメータの編集

「*ネットワーク設定*」エントリは、iRMC S4 の LAN パラメータを設定するページのリンクを提供します。

– 230 ページ の「Network Interface - iRMC S4 上の Ethernet 設定の編集」

– 237 ページ の「ポート番号とネットワークサービス - ポートとネットワークサービスの設定」

– 240 ページ の「DNS 構成 - iRMC S4 の DNS の設定」

7.13.1 Network Interface - iRMC S4 上の Ethernet 設定の編集

「*Network Interface*」ページでは、iRMC S4 のイーサネット設定の表示および変更ができます。

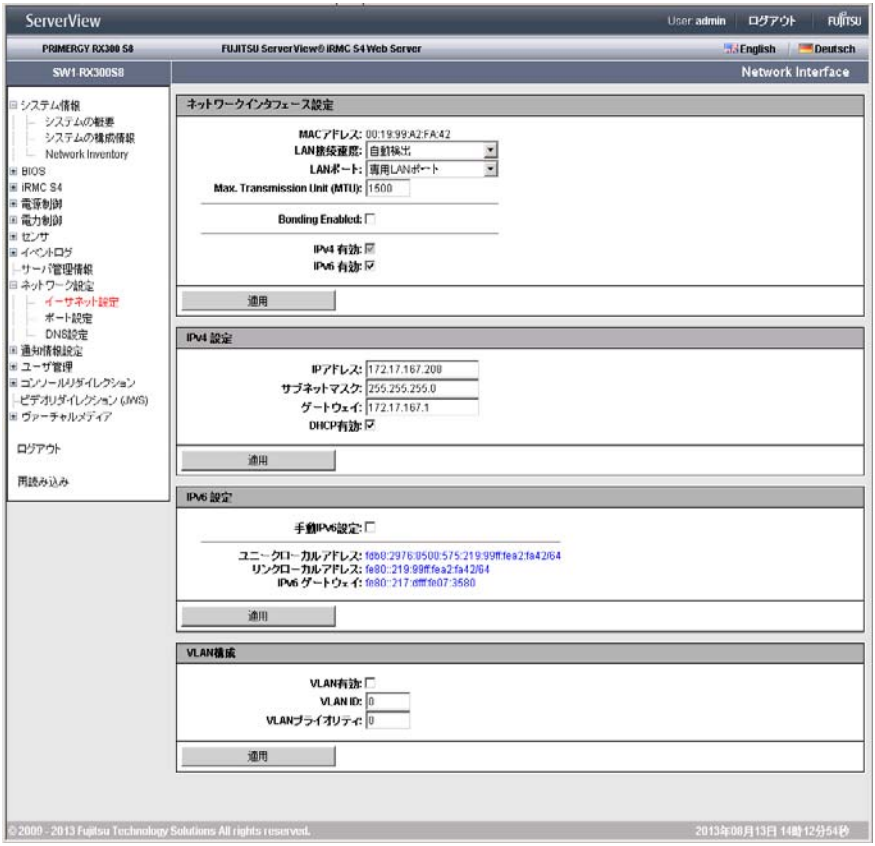


図 133: 「Network Interface」ページ

注意！

イーサネット設定を変更するときは、事前にシステムに責任を持つネットワーク管理者に問い合わせてください。

iRMC S4 のイーサネット設定を誤ると、特別な設定ソフトウェア、シリアルインターフェース、または BIOS を使用しないと iRMC S4 にアクセスできなくなります。

「*iRMC S4 設定*」権限を持つユーザのみが、イーサネット設定を編集することができます（55 ページ の「iRMC S4 のユーザ管理」の章を参照）。

ネットワークインターフェース設定

MAC アドレス

iRMC S4 の MAC アドレスが表示されます。

LAN 接続速度

ネットワークボンディングが有効な場合、このオプションは無効 / 非表示です。

LAN 速度は、以下のオプションを選択できます。

- 自動検出
- 1000 M ビット / 秒 全二重（サーバハードウェアによって異なる）
- 100 M ビット / 秒 全二重
- 100 M ビット / 秒 半二重
- 10 M ビット / 秒 全二重
- 10 M ビット / 秒 半二重

「*自動検出*」を選択すると、、iRMC S4 のオンボード LAN コントローラが、自動的に正しい伝送速度および全二重あるいは半二重方式の接続方法を決定します。

Max. Transmission Unit（MTU）

TCP/IP 接続で許可される TCP/IP データパッケージの最大パケットサイズ（単位 : バイト）（デフォルト : 3000 バイト）。

LAN ポート

> **i** ネットワークボンディングが有効な場合、このオプションは無効 / 非表示です。

NIC（Network Interface Card）システムにインストールされた LAN インターフェースは、以下のいずれかとして設定できます。

– 共用 LAN ポート

または

– 専用 LAN ポート

Bonding Enabled

iRMC S4 のネットワークボンディングを有効 / 無効にします。

iRMC S4 のネットワークボンディングは、Ethernet ネットワーク アダプタの故障時の冗長を目的として設計されています。そのため、iRMC S4 ネットワーク管理のトラフィックは、単一の物理リンクの故障によって発生するサービスロスから保護されます。

iRMC S4 はアクティブバックアップモードのみをサポートします。つまり、リンクが故障するまで一方のポートがアクティブで、リンクが故障するともう一方のポートが MAC を引き継いでアクティブになります。

> **i** ボンディングが有効な場合、「*Active Port*」、「*LAN 接続速度*」、「*LAN ポート*」オプションは無効 / 非表示です。

> **i** iRMC S4 ネットワークボンディングに関連する LAN スイッチは、同じネットワーク内に配置する必要があります。その他に、iRMC S4 ネットワークボンディングには特別なスイッチ設定は必要ありません。

> **i** **なお、次の点に注意してください。**
>
> ネットワークボンディングは、有効な場合でもフロント LAN がアクティブになると保留にされます。フロント LAN ポートはアクティブになり、事前に定義された IP アドレス 192.168.1.1 でアクセスできます。この状況が発生した場合、対応する注記が Web インターフェースに表示されます。
>
> ただし、ボンディングの設定および設定の変更は可能です。フロント LAN が非アクティブ（「リンクダウン」）になると、設定が有効になります。つまり、現在設定されているボンディングの設定に従って、ボンディングモードがアクティブになります。

次の図に、ネットワークボンディングの機能方法の概要を示します

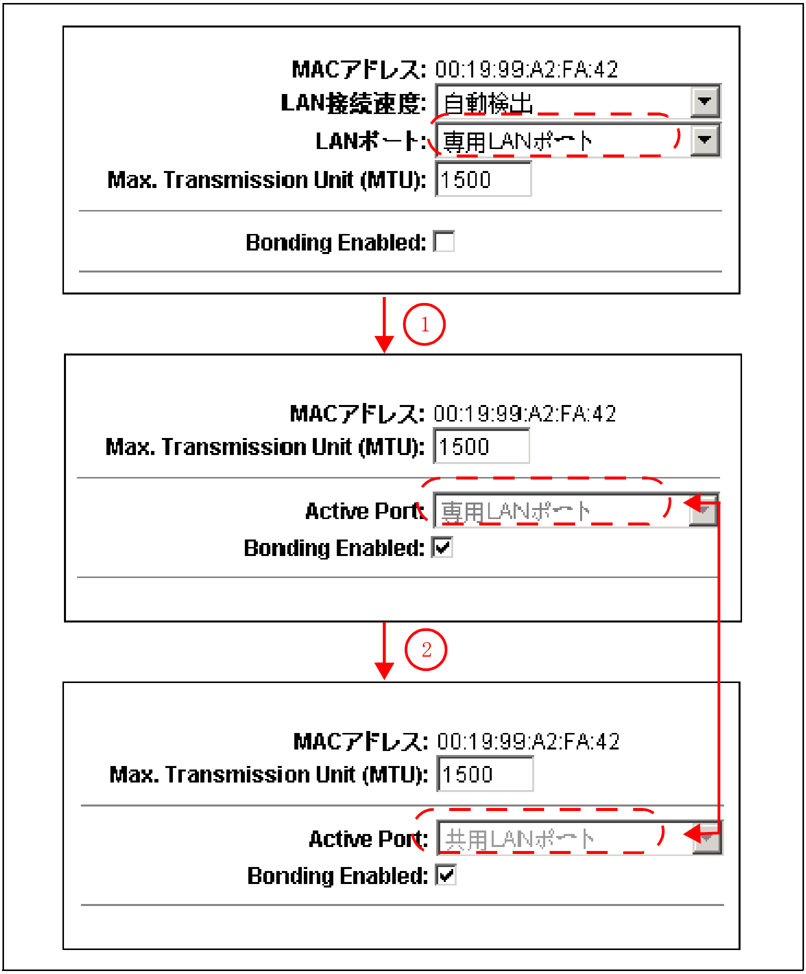


図 134: IP ボンディングの有効化

1. ボンディングがアクティブになると、現在使用されている LAN ポート（ここでは Management LAN）がアクティブポートになり、「*Active Port*」フィールドに表示されます。セカンド LAN ポート（ここではオンボード共有 LAN）がバックアップポートになります。

2. 現在アクティブなポート（ここでは Management LAN）が非アクティブになり（「リンクダウン」）、セカンドポート（ここではオンボード共有 LAN）はアクティブになります。

注意事項：

ブレードサーバは iRMC S4 のボンディングモードをサポートしません。2 つの共有 LAN ポート間に自動フェイルオーバーメカニズムを使用して、冗長ネットワーク機能を保証します。

IPv4 有効

IPv4 ドレッシングは常に iRMC S4 で有効で、無効にすることはできません。

IPv6 有効

iRMC S4 の IPv6 アドレッシングを有効または無効にします。IPv6 アドレッシングを有効にすると「*IPv6 設定*」グループが表示されます（下記参照）。

現在 IPv6 を使用して iRMC S4 にアクセスしている場合は、IPv6 アドレッシングを無効にできません。

IPv4 設定

「*IPv4 設定*」グループでは、iRMC S4 の IPv4 設定を行うことができます。

IP アドレス

LAN 内の iRMC S4 の IPv4 アドレス。このアドレスは管理対象サーバの IP アドレスとは異なります。

静的アドレス（「*DHCP 有効*」オプションが無効）を使用している場合は、ここに IP アドレスを入力できます。そうでない場合（「*DHCP 有効*」オプションが有効）、iRMC S4 ではこのフィールドはアドレスの表示用に使用されます。

サブネットマスク

LAN 内の iRMC S4 のサブネットマスク。

ゲートウェイ

LAN 内のデフォルトゲートウェイの IPv4 アドレス。

DHCP 有効

このオプションを有効にすると、iRMC S4 は、ネットワーク上の DHCP サーバから LAN 設定を取得します。

ネットワーク上に DHCP サーバがない場合は、*DHCP* オプションを有効にしないでください。
DHCP オプションを有効にしてもネットワーク上に DHCP サーバが 存在しない場合、iRMC S4 は検索ループを開始します（つまり、DHCP サーバが見つかるまで検索を続けます）。

（設定された）iRMC S4 は、適切に設定された DHCP サーバによって、DNS サーバ に登録できます。（240 ページ の「DNS 構成 - iRMC S4 の DNS の設定」を参照）

IPv6 設定

「*IPv6 設定*」グループでは、リンクローカルアドレスに加え、iRMC S4 の IPv6 アドレスを手動で設定できます。これは、ステートレス自動設定を使用して、iRMC S4 に常に自動的に割り当てられます。

iRMC S4 の IPv6 アドレッシングを使用する場合、iRMC S4 では DHCP をサポートしません。

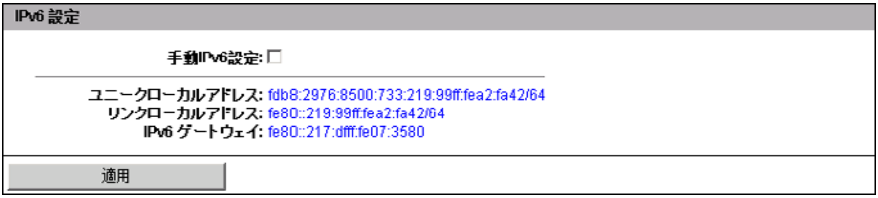


図 135: 「ネットワークインターフェース」ページ - 手動 IPv6 設定無効

手動 IPv6 設定

このオプションはデフォルトでは無効です
「*手動 IPv6 設定*」オプションが有効な場合、「*IPv6 設定*」グループには、iRMC S4 にルータブルな IPv6 アドレスを手動で設定可能な追加のパラメータが表示されます。

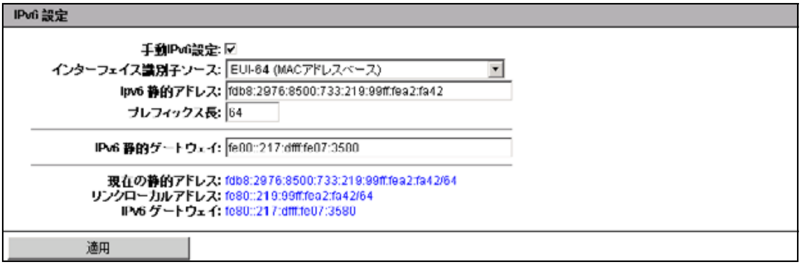


図 136: 「ネットワークインターフェース」ページ - 手動 IPv6 設定

IPv6 静的アドレス
iRMC S4 の静的 IPv6 アドレス。

プレフィックス長
IPv6 プレフィックスの長さ

IPv6 静的ゲートウェイ
LAN 内のデフォルト IPv6 ゲートウェイの静的 IPv6 アドレス。

VLAN 構成

VLAN 有効
このオプションで、iRMC S4 の VLAN サポートを有効にします。

VLAN-ID
iRMC S4 が属する仮想ネットワーク（VLAN ）の VLAN ID。許容される値の範囲 : 1≤ *VLAN ID* ≤ 4094。

VLAN プライオリティ
「*VLAN ID*」で指定した VLAN における iRMC S4 の VLAN プライオリティ。
許容される値の範囲 : 0 ≤ *VLAN プライオリティ* ≤ 7（デフォルト : 0)。

7.13.2 ポート番号とネットワークサービス - ポートとネットワークサービスの設定

「*ポート番号とネットワークサービス*」ページでは、ポート番号およびネットワークサービスの表示および設定ができます。

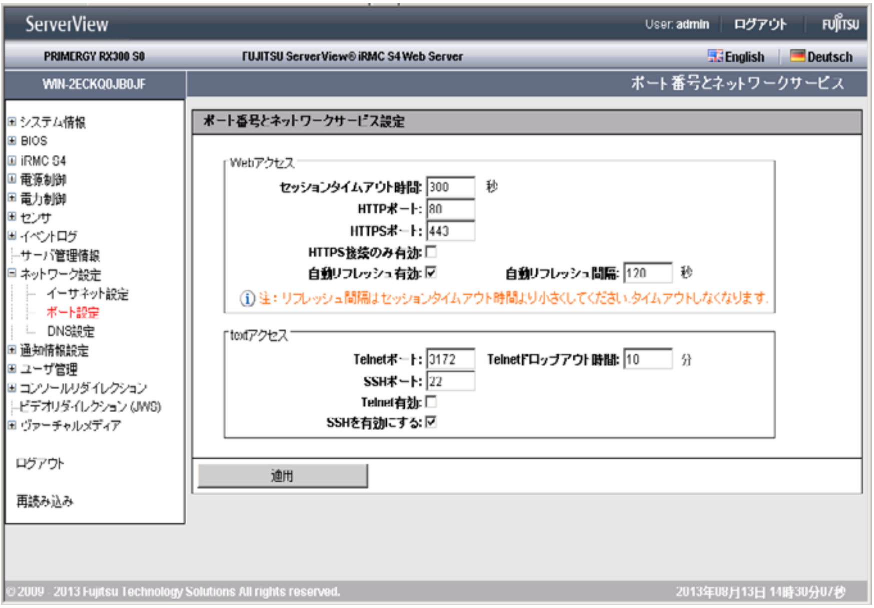


図 137: 「ポート番号とネットワークサービス」ページ

> **i** 入力フィールドが iRMC S4 Web インターフェースで無効な場合、ポート番号の設定はサポートされません。

Web アクセス

セッションタイムアウト時間

通信していない期間（秒）が設定値を経過すると自動的にセッションが閉じられます。iRMC S4 Web インターフェースのログインページが表示され、再びログインするように求められます（120 ページを参照）。

> i 「*セッションタイムアウト*」より短いリフレッシュ間隔を「*自動リフレッシュ間隔*」フィールドに入力した場合、「*セッションタイムアウト*」に設定された時間が経過してもセッションは自動的に閉じません（239 ページを参照）。

HTTP ポート

iRMC S4 の HTTP ポート
デフォルトポート番号 : 80
変更可能 : 可能
デフォルトで有効 : 対応
通信方向 : inbound および outbound

HTTPS ポート

iRMC S4 の HTTPS (HTTP Secure) ポート
デフォルトポート番号 : 443
変更可能 : 可能
デフォルトで有効 : 対応
通信方向 : inbound および outbound

HTTPS 接続のみ有効

「*HTTPS 接続のみ有効*」オプションを有効にした場合、入力フィールドに指定した HTTPS ポートでのみ iRMC S4 への安全な通信を確立することができます。

「*HTTPS 接続のみ有効*」オプションを無効にした場合、入力フィールドに指定した HTTP ポートで iRMC S4 への非安全な通信を確立することができます。

> i SSL 証明書の期限が切れていると、その旨のメッセージがブラウザに出されます。

自動リフレッシュ有効

このオプションを有効にすると、iRMC S4 Web インターフェースの画面は、自動的に周期的に再読み込みされます。「*自動リフレッシュ間隔*」フィールドに、再読み込みの間隔を設定します。

自動リフレッシュ間隔

iRMC S4 Web インターフェースが、自動的に再読み込みする間隔（秒）を設定します。

> **i** 再読み込み間隔の値に「*セッションタイムアウト*」（238 ページを参照））よりも短い時間を設定した場合、セッションは、「*セッションタイムアウト*」を経過しても自動的に閉じません。

text アクセス

Telnet ポート

iRMC S4 の Telnet ポート
デフォルトポート番号：3172
変更可能 : 可能
デフォルトで有効 : 非対応
通信方向 : inbound および outbound

Telnet ドロップアウト時間

通信がなされないとき Telnt/SSH 接続が自動的に切断されるまでの時間（秒）。

SSH ポート

iRMC S4 の SSH（Secure Shell）ポート
デフォルトポート番号：２２
変更可能 : 可能
デフォルトで有効 : 対応
通信方向 : inbound および outbound

Telnet 有効

「*Telnet 有効*」オプションを有効にした場合、ユーザは、入力フィールドに指定した TELNET ポートで、iRMC S4 への接続を確立することができます。

SSH を有効にする

「*SSH を有効にする*」オプションを有効にした場合、ユーザは、入力フィールドに指定した SSH ポートで、iRMC S4 への接続を確立することができます。

▶ *「適用」*ボタンをクリックして、編集された設定を保存してください。

7.13.3 DNS 構成 - iRMC S4 の DNS の設定

「*DNS 構成*」ページでは、iRMC S4 のドメインネームサービス（DNS）を有効にして、iRMC S4 のホスト名を設定できます。

図 138: 「DNS 構成」ページ

DNS 設定

「*DNS 設定*」グループで、iRMC S4 のドメインネームサービス（DNS）を有効にできます。これによって、iRMC S4 の設定に IP アドレスではなく具体的な DNS 名を使用できます。

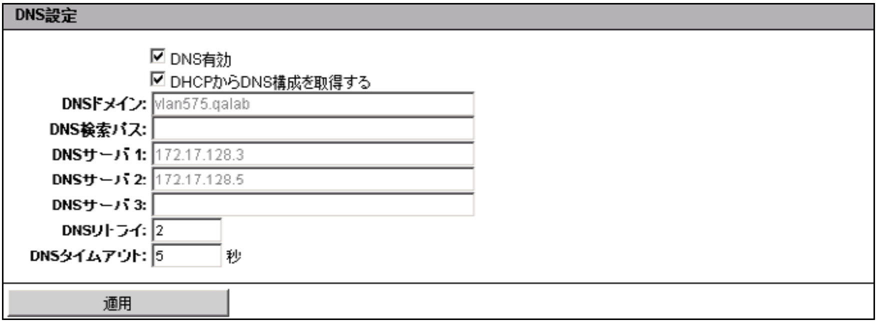


図 139: 「DNS 構成」ページ - DNS 設定

DNS 有効

iRMC S4 の DNS を有効 / 無効にします。

DHCP から DNS 構成を取得する

このオプションをアクティブにすると、DNS サーバの IP アドレスは DHCP サーバから自動的に取得されます。
この場合、最大 3 つの DNS サーバに対応します。

この設定を有効にしない場合、「*DNS サーバ 1*」から「*DNS サーバ　3*」に最大 3 つの DNS サーバアドレスを入力できます。

DNS ドメイン

「*DHCP から DNS 構成を取得する」オプションが無効な場合、DNS サーバへの要求に対するデフォルトドメインの名前を指定します。*

DNS 検索パス

1 つ以上のスペース文字で区切られる（部分的修飾）ドメイン名のリスト。DNS 検索リストは、最大 256 文字まで有効です。ドメイン名コンポーネントを含まないホスト名を検索する場合は、「DNS Search Path」フィールドを使用して検索するドメインを指定します。

DNS サーバ 1　..3

「*DHCP から DNS 構成を取得する*」オプションが無効な場合、ここで、最大 5 つの DNS サーバ名を入力できます。

DNS リトライ

DNS リトライ回数。

DNS タイムアウト
DNS 応答のタイムアウト（秒）。

▶ *「適用」*ボタンをクリックして、編集された設定を保存してください。

DNS 登録名

「*DNS 名*」グループでは、iRMC S4 のホスト名を設定でき、「動的 DNS」を使用できます。動的 DNS によって、DHCP サーバはネットワークコンポーネントの IP アドレスとシステム名を DNS サーバに自動的に渡して、識別を容易にできます。

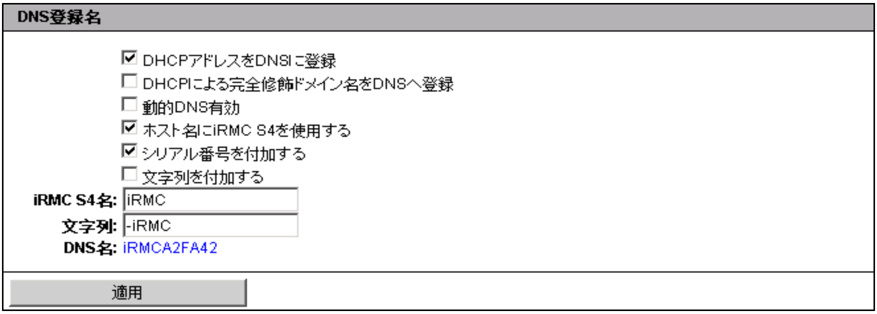


図 140: 「DNS 構成」ページ - DNS 名

DHCP アドレスを DNS に登録
このオプションは、IPv6 アドレッシングを使用する場合は無効です。DHCP サーバを使用して iRMC S4 と DNS を登録するための、DHCP サーバへの DHCP 名の転送を有効または無効にします。

DHCP による完全修飾ドメイン名を DNS へ登録
このオプションは、IPv6 アドレッシングを使用する場合は無効です。DHCP サーバを使用して iRMC S4 と DNS を登録するための、DHCP サーバへの FQDN（完全修飾ドメイン名）の転送を有効または無効にします。

動的 DNS 有効
動的 DNS を使用した DNS レコードのアップデートを有効または無効にします。

i 非安全な DNS のみサポートされます。

ホスト名に iRMC S4 を使用する

「*iRMC S4 Name*」入力フィールドに指定された iRMC S4 名が、サーバ名の代わりに iRMC S4 に使用されます。

シリアル番号を付加する

iRMC S4 の MAC アドレスの最後の 3 バイトが iRMC S4 の DHCP 名に付加されます。

文字列を付加する

「*Extension*」入力フィールドに指定された拡張子が、iRMC S4 の DHCP 名に付加されます。

iRMC S4 名

サーバ名の代わりに、iRMC 向け DHCP に渡された iRMC S4 名。関連するオプションによって異なりますが、iRMC S4 名が DNS 名の一部として使用されます。

文字列

iRMC S4 の名前の拡張子。

DNS 名

iRMC S4 に設定された DNS 名を表示します。

► *「適用」*ボタンをクリックして、編集された設定を保存してください。

7.14 通知情報設定 - 警告通知の設定

「*通知情報設定*」エントリには、iRMC S4 の警告通知の設定を行う際に利用するページのリンクがあります。

– 245 ページ の「SNMP トラップ送信設定 - SNMP トラップ通知の設定」

– 246 ページ の「Email 設定 - Email 送信設定」

7.14.1 SNMP トラップ送信設定 - SNMP トラップ通知の設定

「*SNMP トラップ送信設定*」ページでは、SNMP トラップ通知の設定の表示および構成ができます。

> **i** SNMP トラップを最大 7 つの SNMP サーバに送信する機能をサポートしています

図 141: 「SNMP トラップ送信設定」ページ

SNMP コミュニティ

SNMP コミュニティ名。

► 「*適用*」をクリックしてコミュニティ名を受け入れます。

「SNMP サーバ 1」～「SNMP サーバ 7」（トラップ送信先）

コミュニティに属し、「*トラップ送信先*」を設定するサーバの DNS 名または IP アドレス。

► 「*適用*」ボタンをクリックして、トラップの送信先として SNMP サーバを有効にします。

► 「*TFTP テスト*」をクリックすると、SNMP サーバへの接続をテストします。

▶ 「*すべて適用*」ボタンをクリックすると、適切な場合、すべての設定が有効になります。

7.14.2 Email 設定 - Email 送信設定

「*Email 設定*」ページを使用して、Email 通知の設定を行うことができます。

> **i** 2 つのメールサーバの設定がサポートされます。
>
> Email 通知は各ユーザに個別に指定できます（255 ページ の「「ユーザ “<name>” 構成」- ユーザ設定（詳細）」の項を参照）。

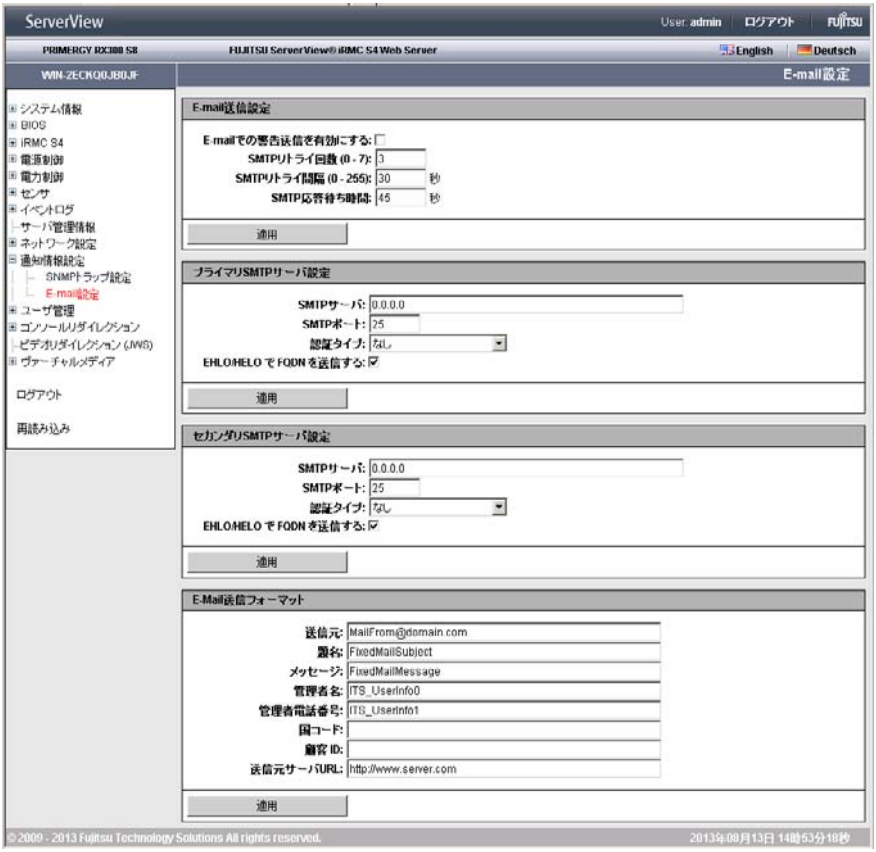


図 142: 「Email 設定」ページ

E-mail 送信設定 - グローバル Email 設定

「*E-mail 送信設定*」グループでは、グローバル Email 設定を設定できます。

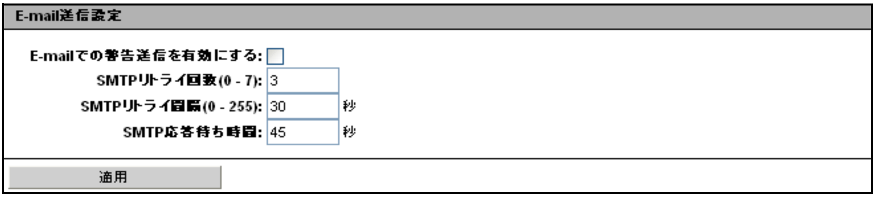


図 143: 「Email 設定」ページ - グローバル Email 設定

E-mail での警告送信を有効にする。
このオプションを有効にします。

SMTP リトライ回数（0 - 7）
SMTP リトライ回数。

SMTP リトライ間隔（0 - 255）
SMTP 再試行の間隔（秒）。

SMTP 応答待ち時間
SMTP 応答のタイムアウト（秒）。

▶ 「*適用*」をクリックすると設定が有効になります。

プライマリ SMTP サーバ設定 - プライマリメールサーバの設定

「*プライマリ SMTP サーバ設定*」グループを使用して、プライマリサーバ（SMTP サーバ）の設定を行うことができます。

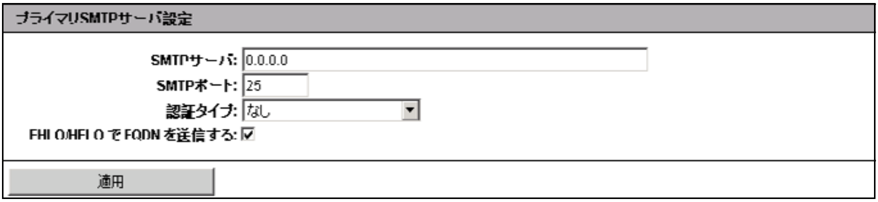


図 144: 「E-mail 設定」ページ - プライマリ SMTP サーバ設定

SMTP サーバ
プライマリメールサーバの IP アドレス。

iRMC S4 のドメインネームシステム（DNS）を有効にできます
（240 ページ の「DNS 構成 - iRMC S4 の DNS の設定」を参照）。
IP アドレスの代わりに、具体的な名前を使用できます。

SMTP ポート
メールサーバの SMTP ポート番号。

認証タイプ
iRMC S4 をメールサーバに接続する際の認証方式を選択します。

– *なし*
接続に認証を使用しません。

– *認証を行う (RFC 2554)*
SMTP 認証（RFC 2544 ）RFC 2554 に準拠した認証方式 : SMTP サーバの認証方式の拡張です。

この場合は、以下の情報が必要です。

認証ユーザ名
メールサーバでの認証用のユーザ名。

認証パスワード
メールサーバでの認証用のパスワード。

パスワード確認
入力したパスワードを確定します。

EHLO/HELO で FQDN を送信する
EHLO/HELO を使用して FDQN を有効 / 無効にします。

▶ 「*適用*」をクリックすると設定が有効になります。

セカンダリ SMTP サーバ設定 - セカンダリメールサーバ設定

「*セカンダリ SMTP サーバ設定*」グループを使用して、セカンダリサーバ（SMTP サーバ）の設定ができます。

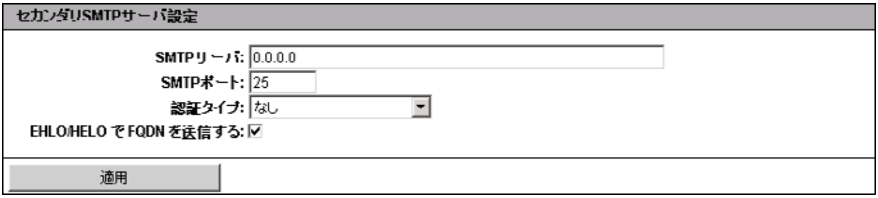


図 145: 「E-mail 設定」ページ - セカンダリ SMTP サーバ設定

SMTP サーバ

セカンダリメールサーバの IP アドレス。

> iRMC S4 のドメインネームシステム（DNS）を有効にできます（240 ページ の「DNS 構成 - iRMC S4 の DNS の設定」を参照）。IP アドレスの代わりに、具体的な名前を使用できます。

SMTP ポート

メールサーバの SMTP ポート番号。

認証タイプ

iRMC S4 をメールサーバに接続する際の認証方式を選択します。

– *なし*
  接続に認証を使用しません。

– *SMTP AUTH (RFC 2554)*
  SMTP 認証（RFC 2544 ）RFC 2554 に準拠した認証方式 : SMTP サーバの認証方式の拡張です。

  この場合は、以下の情報が必要です。

  認証ユーザ名
  メールサーバでの認証用のユーザ名。

  認証パスワード
  メールサーバでの認証用のパスワード。

  パスワード確認
  入力したパスワードを確定します。

EHLO/HELO で FQDN を送信する
EHLO/HELO を使用して FDQN を有効 / 無効にします。

▶ 「*適用*」をクリックすると設定が有効になります。

E-mail 送信フォーマット -
電子メール送信フォーマットの設定

「*E-mail 送信フォーマット*」グループでは E-mail フォーマット設定を行うことができます。個々のユーザについて「*新規ユーザの設定*」-「*ユーザ < 名 > 設定*」-「*E-mail 送信フォーマット*」ページを使用して E-mail フォーマットを設定できます（259 ページ参照）。

以下の Email フォーマットがサポートされています。

– 標準
– 題名固定
– ITS フォーマット

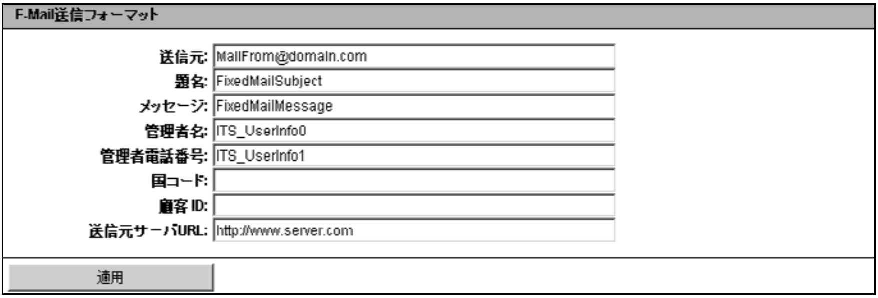


図 146: 「E-mail 設定」ページ - E-mail 送信フォーマット

E-mail フォーマットによっては、入力できない項目があります。

送信元
iRMC S4 送信者を識別する情報です。
すべての電子メール形式に対して有効です。

i ここで入力した文字列に「@」が含まれている場合、文字列は有効な E-mail アドレスと解釈されます。そうでない場合、有効な Email アドレスとして「admin@<ip-address>」が使用されます。

題名

アラートメールの固定件名。
「*決定されたフォーマット*」の電子メール形式についてのみ有効です。
（259 ページ）

メッセージ

メッセージのタイプ（E-mail）。
「*決定されたフォーマット*」の電子メール形式についてのみ有効です。
（259 ページ）

管理者名

担当の管理者名（オプション）。
ITS メール形式についてのみ有効です。（259 ページ）

管理者電話番号

担当の管理者の電話番号（オプション）。
ITS メール形式についてのみ有効です。（259 ページ）

国コード

ISO 3166 ISO 3166 alpha 2 に基づくアルファベット 2 文字の国コード。

顧客 ID

顧客識別子。

送信元サーバ URL

特定の条件で、サーバがアクセスできる URL。URL を手動で入力する必要があります。
Standard メール形式についてのみ有効です。

► 「*適用*」をクリックすると設定が保存します。

7.15 ユーザ管理

「*ユーザ管理*」エントリには、ローカルユーザ管理のページだけでなく、グローバルユーザ管理のディレクトリサービスを設定（LDAP 設定）するためのページへのリンクが含まれます。

– 252 ページ の「ユーザ管理 - iRMC S4 のローカルユーザ管理」

– 262 ページ の「ディレクトリサービス構成 - iRMC S4 でディレクトリサービスの設定」

– 276 ページ の「Centralized Authentication Service（CAS）設定 - CAS サービスの設定」

7.15.1 ユーザ管理 - iRMC S4 のローカルユーザ管理

*「ユーザ管理」*ページには、設定されたユーザに関する情報が表示されます。各行には、設定された特定のユーザに関するデータが含まれます。ユーザ名はリンク形式で実装されています。
ユーザ名をクリックして「*ユーザ "<name>" 設定*」ウィンドウを開くと（255 ページを参照）、そのユーザの設定を表示したり変更することができます。

i ユーザ ID 1（"null user"）は、IPMI 標準のために予約されているため、iRMC S4 のユーザ管理には使用できません。

図 147: 「ユーザ管理」ページ

削除

設定されているユーザの表には、各ユーザエントリの後に「*削除*」ボタンがあります。このボタンをクリックして、選択を確認した後に関連するユーザを削除します。

ユーザの新規作成

このボタンをクリックすると、「*新規ユーザの構成*」ページが開きます（254 ページを参照）。ここで新規ユーザの設定ができます。

7.15.1.1　新規ユーザの構成 - 新規ユーザの構成

「*新規ユーザの構成*」ページを使用して、新規ユーザの基本設定ができます。

「*新規ユーザの構成*」ページのフィールドと選択肢の一覧については、256 ページ の「*ユーザ “<name>” 設定*」ページで説明します。

In 図 148 に、「user3」という名前のユーザの設定を示します。

図 148: 「ユーザ管理」- 「新規ユーザの構成」ページ

7.15.1.2 「ユーザ “<name>” 構成」- ユーザ設定（詳細）

「*ユーザ “<name>” 構成*」ページでは、ユーザ設定の表示、修正および拡張ができます。

図 149 に、図 148 で作成したユーザの設定を示します。

> **i** ユーザ名の後ろの括弧内にユーザ ID が表示されます。

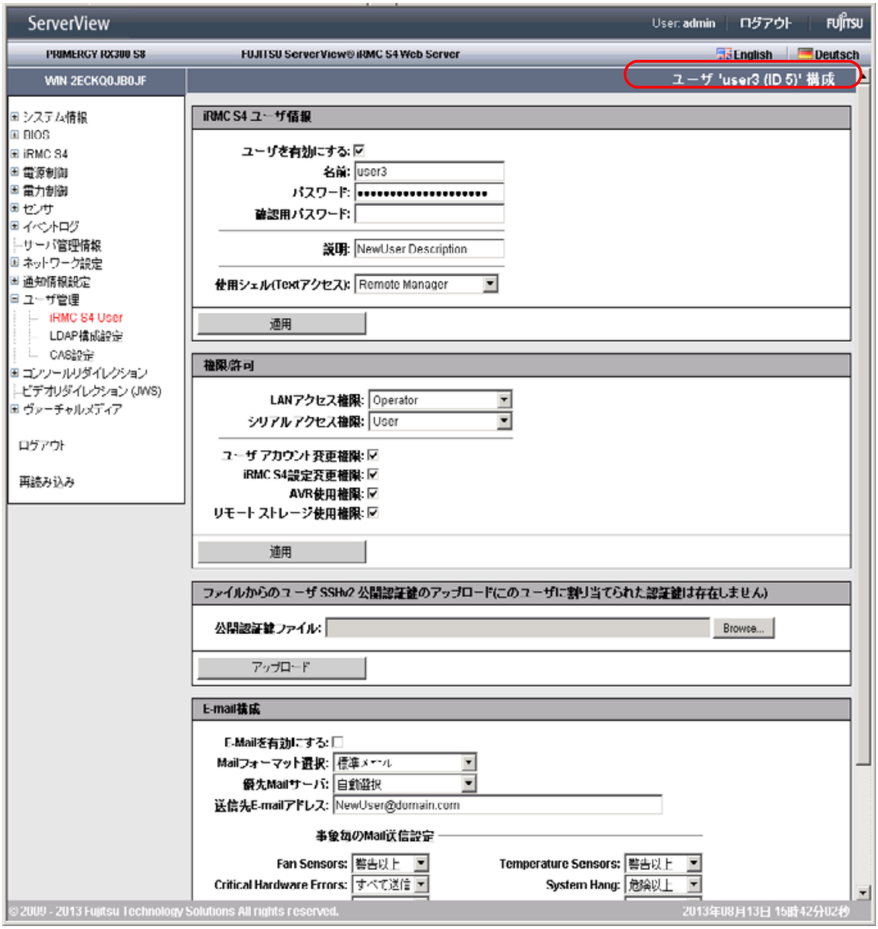


図 149: 「ユーザ管理」- 「ユーザ “<name>”」

iRMC S4 ユーザ情報 - ユーザのアクセスデータの設定

「*iRMC S4 ユーザ情報*」グループでは、ユーザのアクセスデータを設定できます。

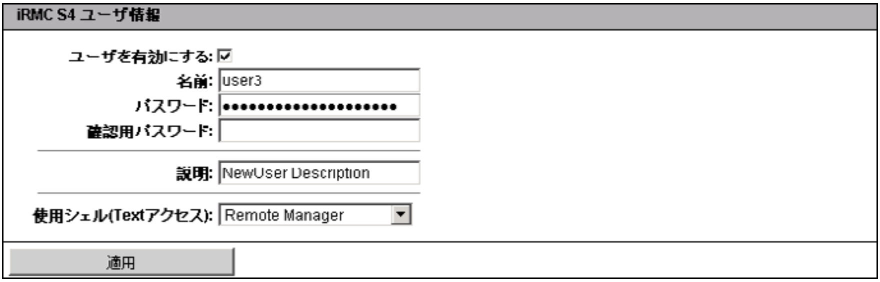


図 150: 「ユーザ管理」- 「ユーザ “<name>” 構成」ページ、「iRMC S4 ユーザ情報」

ユーザを有効にする

このオプションを無効に設定するとユーザをロックできます。

名前

ユーザの名前を入力します。

> i 有効なユーザ名はアルファベットで開始する必要があります。名前の残りの部分には、アルファベット、数字、アンダーバー、ダッシュ、ピリオド、アットマーク（@）のみ含めることができます。
>
> 空白文字は使用できません。

> i ユーザ名は一意である必要があります。ユーザ名の重複はできません。

パスワード

ユーザパスワードを入力します。

確認用パスワード

パスワードを再度入力して、確認します。

説明

構成したユーザの一般的な説明を入力します。

使用シェル (Text アクセス)
目的のユーザシェルを選択します。
以下のオプションを選択できます。

– *SMASH CLP*
325 ページ の「コマンドラインシェルの起動 ...- SMASH CLP シェルの起動」の項を参照してください。

– *Remote Manager*
303 ページ の「Telnet/SSH 経由の iRMC S4 (リモートマネージャ)」の章を参照してください。

– *IPMI Terminal Mode*

– *None*

▶ 「*適用*」をクリックすると設定が有効になります。

権限 / 許可 - ユーザ権限の設定

「*権限 / 許可*」グループを使用して、チャネル固有のユーザ権限を設定できます。

図 151: 「ユーザ管理」- 「ユーザ “<name>” 構成」ページ、「権限 / 許可」

LAN アクセス権限
ここで LAN チャネルの権限グループをユーザに割り当てます。

– *User*
– *Operator*
– *Administrator*
– *OEM*

権限グループに関連する許可に関する情報は、55 ページ の「iRMC S4 のユーザ管理」の章 を参照してください。

シリアルアクセス権限

ユーザへのシリアルチャネルの権限グループを割り当てます。「*LAN アクセス権限*」についても同じ権限グループを使用できます。

チャネル別許可に加えて、次のチャネル非依存許可を個別にユーザに割り当てることもできます。

ユーザアカウント変更権限

ローカルユーザアクセスデータを設定する権限。

iRMC S4 設定変更権限

iRMC S4 設定を行う権限。

AVR 使用権限

「View Only」および「フルコントロール」モードで AVR（ビデオリダイレクション）を使用する権限。

リモートストレージ使用権限

リモートストレージ機能を使用する権限。

▶ 「*適用*」をクリックすると設定が有効になります。

ファイルからのユーザ SSHv2 公開認証鍵のアップロード

「*ファイルからのユーザ SSHv2 公開認証鍵のアップロード*」グループを使用して、ローカルファイルからユーザの SSHv2 公開鍵をアップロードすることができます。

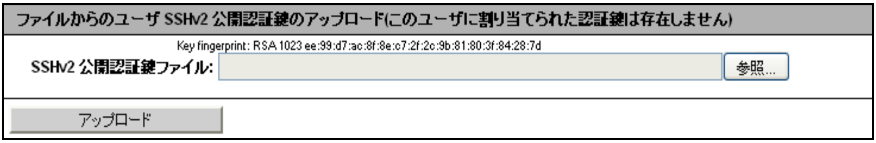


図 152: 「ユーザ管理」- 「ユーザ “<name>” 構成」ページ、「ファイルからのユーザ SSHv2 公開認証鍵のアップロード」

iRMC S4 ユーザの SSHv2 公開鍵認証の詳細については、67 ページ の「SSHv2 鍵のファイルから iRMC S4 へのアップロード」の項を参照してください。

E-mail 構成 - ユーザ固有の E-mail 設定

「*E-mail 構成*」グループを使用して、ユーザ固有の E-mail フォーマットを行うことができます。

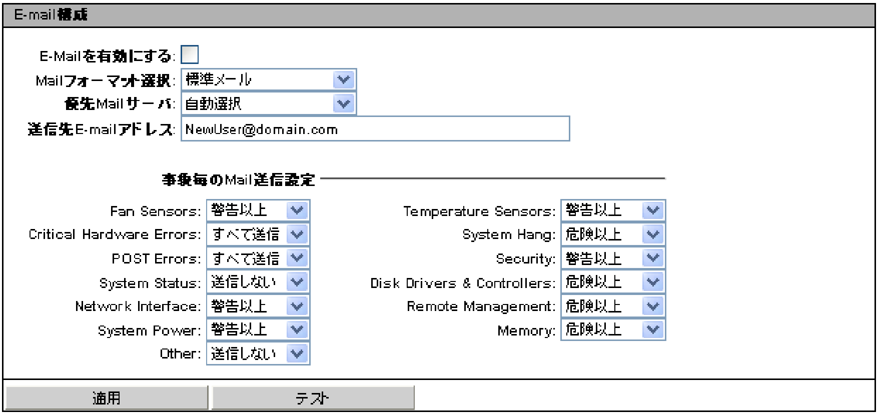


図 153: 「ユーザ管理」- 「ユーザ “<name>” 設定」ページ、「E-mail 構成」

E-mail を有効にする

システムステータスを Email でユーザに通知するかどうかを指定します。

Mail フォーマット選択

選択された E-mail フォーマットによって、「*E-mail 通知 – E-mail フォーマットの設定*」グループで設定を行うことができます（250 ページを参照）。

以下の E-mail フォーマットを使用できます。

– *標準メール*
– *題名固定*
– *ITS フォーマット*

優先 Mail サーバ
優先メールサーバを選択します。
以下のオプションの 1 つを選択できます。

– *自動選択*

プライマリメールサーバが稼動していない場合など、電子メールが即座に正常に送信できない場合、電子メールはセカンダリメールサーバに送信されます。

– *プライマリ*

プライマリ SMTP サーバとして設定されたメールサーバ（247 ページ を参照）だけが、優先メールサーバとして使用されます。

– *セカンダリ*

セカンダリ SMTP サーバとして設定されたメールサーバ（249 ページ を参照）だけが、優先メールサーバとして使用されます。

i Email 送信のエラーはイベントログに記録されます。

送信先 E-mail アドレス
受信者の Email アドレス。

事象毎の Mail 送信設定

iRMC S4 ユーザに Email で通知するシステムイベントを設定できます。

> **i** iRMC S4 のイベントログの各エントリは、特定の通知グループに割り当てられます。

各イベントグループについて、以下の設定を使用できます。

なし

このページンググループについては、通知機能は無効になります。

危険以上

システムイベントログに「*CRITICAL*」と記録されたエントリがある場合、Email で通知されます。

警告

システムイベントログに「*Minor*」、「*Major*」、「*Critical*」のいずれかが記録されたエントリがある場合、Email で通知されます。

すべて送信

エントリがシステムイベントログに記録されたグループの全てのエントリが通知されます。

► 「*適用*」をクリックすると設定が有効になります。

7.15.2 ディレクトリサービス構成 - iRMC S4 でディレクトリサービスの設定

ディレクトリサービスでグローバルユーザ管理を行うには（『ServerView でのユーザ管理』マニュアルを参照）、「*ディレクトリサービス構成*」ページで iRMC S4 を適切に設定する必要があります。

> **i** 現在 iRMC S4 LDAP がサポートするディレクトリサービスは、Microsoft Active Directory、Novell eDirectory および Open LDAP です。

> **i** 以下の記号は、LDAP 上で文字列を検索するためのメタキャラクタとして予約されています : *、\ 、&、|、!、=、<、>、~、:
>
> したがって、ユーザはこれらの文字を相対識別名（RDN）の要素として使用することはできません。

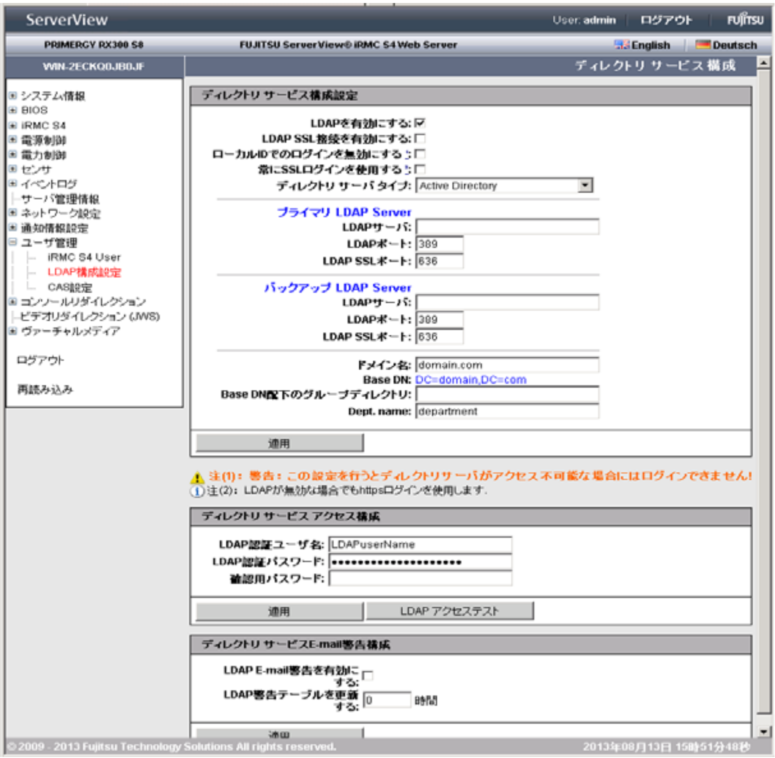


図 154: 「ディレクトリサービス構成」ページ（LDAP 構成）

LDAP を有効にする

このオプションで、iRMC S4 が、LDAP を使用してディレクトリサービスにアクセスできるか否かを設定します。LDAP を使用するディレクトリサービスへのアクセスは、「*LDAP を有効にする*」が有効な場合のみ有効です。

「*LDAP を有効にする*」が有効な場合（120 ページを参照）、ログイン情報は、常に SSL 暗号化されて Web ブラウザと iRMC S4 の間で送信されます。

LDAP SSL 接続を有効にする

このオプションが有効な場合、iRMC S4 とディレクトリサーバ間のデータ送信は SSL 暗号化されます。

「*LDAP SSL 接続を有効にする*」は、iRMC S4 Web インターフェースページが開くときに SSL 保護するかどうかには影響ありません。

「*LDAP SSL 接続を有効にする*」は、ドメインコントローラ認証がインストールされている場合にしか有効にできません。

ローカル ID でのログインを無効にする

このオプションを有効にした場合、iRMC S4 のローカルユーザ認証はロックされ、ディレクトリサービスによるユーザ認証のみが有効になります。

注意！

「*ローカル ID でのログインを無効にする*」が有効になっていて、ディレクトリサービスへの接続が不可能な場合、iRMC S4 へのログインはできなくなります。

常に SSL ログインを使用する

このオプションは LDAP を無効にした場合にのみ有効です。

このオプションを有効にすると、LDAP が無効にされていても、常に HTTP SSL セキュアなログインページが使用されます。「*常に SSL ログインを使用する*」を有効にせず、かつ、LDAP が無効になっている場合は、簡易ユーザ認証がログインに使用されます。

ディレクトリサーバタイプ

使用するディレクトリサーバのタイプ。

以下のディレクトリサービスがサポートされます。

– *Active Directory* : Microsoft Active Directory
– *Novell* : Novell eDirectory
– *OpenLDAP* : OpenLDAP
– *Open DS /Open DJ*

▶ 「*適用*」をクリックすると設定が有効になります。

選択するディレクトリサービスによって、表示される入力フィールドが異なります。

– 「*Active Directory*」については、265 ページ の「Microsoft Active Directory 用の iRMC S4 の設定」の項を参照してください。

– 「*eDirectory*」、「*Open LDAP*」、「*OpenDS DJ*」については、269 ページ の「iRMC S4 の Novell eDirectory/OpenLDAP/OpenDS/Open DJ のための設定」の項を参照してください。

7.15.2.1 Microsoft Active Directory 用の iRMC S4 の設定

選択した「*Active Directory*」を確定後「*適用*」をクリックすると、次の仕様の「*ディレクトリサービス構成*」ページが表示されます。

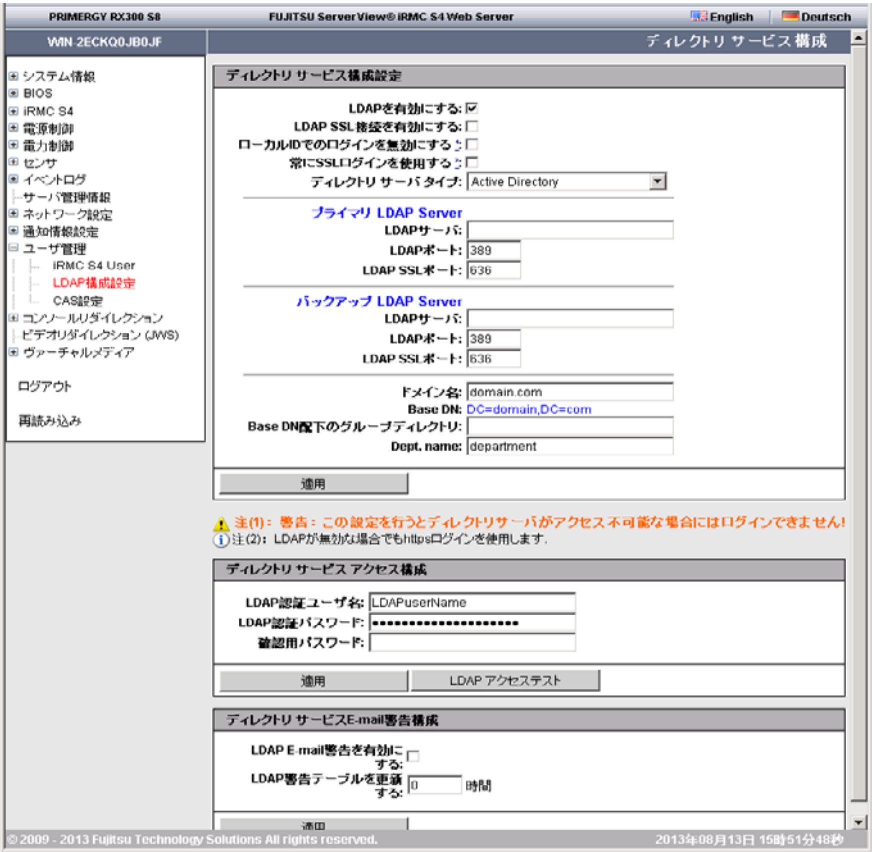


図 155: ディレクトリサービス構成 : Microsoft Active Directory の仕様

> **i** で例として表示されるエントリは 図 155 に示す例および図を参照しています。

次の手順に従います。

► 「*ディレクトリサービス構成設定*」グループの設定を完成させせます。

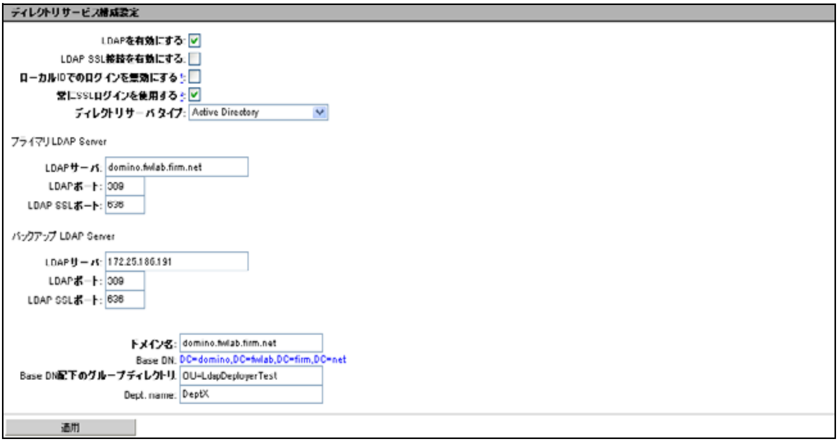


図 156: 「ディレクトリ サービス構成」ページ - ディレクトリサービス構成設定 : Microsoft Active Directory の仕様

プライマリ LDAP Server
: 使用する LDAP ディレクトリサーバ。

LDAP サーバ
: プライマリ LDAP サーバの IP アドレスまたは DSN 名。

LDAP ポート
: プライマリ LDAP サーバの LDAP ポート。

LDAP SSL ポート
: プライマリ LDAP サーバのセキュアな LDAP ポート。

バックアップ LDAP Server
: バックアップサーバとして運用され、「*LDAP サーバ 1*」が故障した場合のディレクトリサーバとして使用される LDAP ディレクトリサーバ。

LDAP サーバ
: バックアップ LDAP サーバの IP アドレスまたは DSN 名。

LDAP ポート
: バックアップ LDAP サーバの LDAP ポート。

LDAP SSL ポート
: バックアップ LDAP サーバのセキュアな LDAP ポート。

ドメイン名
ディレクトリサーバの完全な DNS パス名。

Base DN
「*Base DN*」は、「*ドメイン名*」から自動的に取得されます。

Base DN 配下のグループディレクトリ
Base DN（Group DN Context）のサブツリーとして *SVS* または *iRMCgroups* を含む組織単位（OU）のパス名。

Dept. name
「Dept. name」は、ディレクトリサービスではユーザ許可と警告ロールを確認するために使用されます。Department X サーバと Department Y サーバでは、許可が異なることがあります。

▶ 「*適用*」をクリックすると設定が有効になります。

▶ 「*ディレクトリサービスアクセス構成*」グループで、LDAP アクセスデータを設定します。

ℹ ここで行う設定は、グローバルユーザ ID に関連する警告通知のために必要なものです。警告通知が無効な場合、「*ディレクトリサービスアクセス構成*」は重要ではありません。

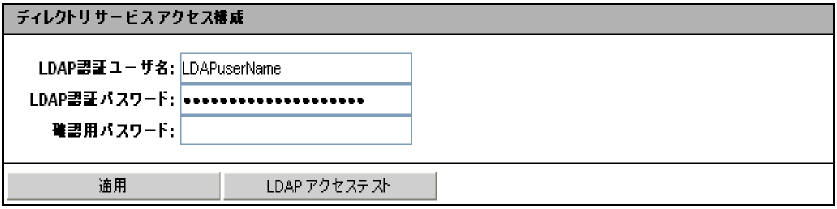


図 157: 「ディレクトリ サービス構成」ページ - ディレクトリサービスアクセス構成 : Microsoft Active Directory

LDAP 認証ユーザ名
LDAP サーバにログオンするときの iRMC S4 ユーザ名。

LDAP 認証パスワード
ユーザ名の下に指定したパスワードを使用して、LDAP サーバでの認証を行います。

確認用パスワード
「*LDAP 認証パスワード*」に入力したパスワードをもう一度入力します。

LDAP アクセステスト

LDAP ディレクトリサーバへのアクセスデータをチェックし、LDAP の状態をその結果として表示します（図 158 を参照）。

> **i** このテストは基本的なアクセスデータ（「LDAP サーバが存在するか」あるいは「ユーザは設定されているか」）を確認するもので、ユーザ認証のすべてを確認するものではありません。

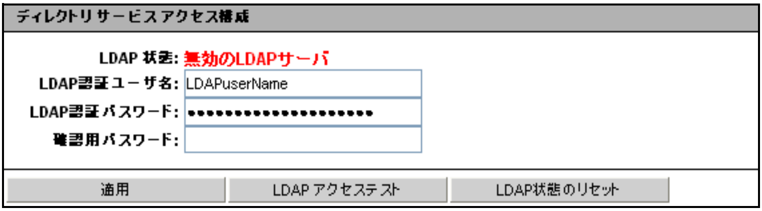


図 158: 「ディレクトリ サービス構成」ページ - サーバの接続状況 : Microsoft Active Directory

- 「*LDAP 状態のリセット*」ボタンをクリックして、画面への表示をリセットします。

- 「*適用*」をクリックすると設定が有効になります。

- 「*ディレクトリサービス E-mail 警告構成*」グループを使用して、グローバル Email 警告の設定を行います。

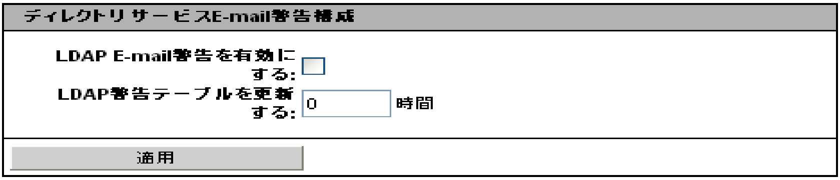


図 159: 「ディレクトリ サービス構成」ページ - ディレクトリサービス E-mail 警告構成

LDAP E-mail 通知を有効にする

グローバル Email 通知を有効にします。

LDAP 警告テーブルを更新する（時間）

Email テーブルを定期的に更新する間隔を定義します（『ServerView でのユーザ管理』を参照）。

> **i** 0 よりも大きい値を指定することを推奨します。「0」を設定すると、テーブルは定期的に更新されなくなります。

► 「*適用*」をクリックすると設定が有効になります。

7.15.2.2 iRMC S4 の Novell eDirectory/OpenLDAP/OpenDS/Open DJ のための設定

「*適用*」をクリックして「*Novell*」または「*OpenLDAP*」を選択すると、「*ディレクトリサービス構成*」ページが表示されます。

i 「*ディレクトリサービス構成*」ページの構造は、Novell eDirectory、OpenLDAP、OpenDS/OpenDJ では同じです。

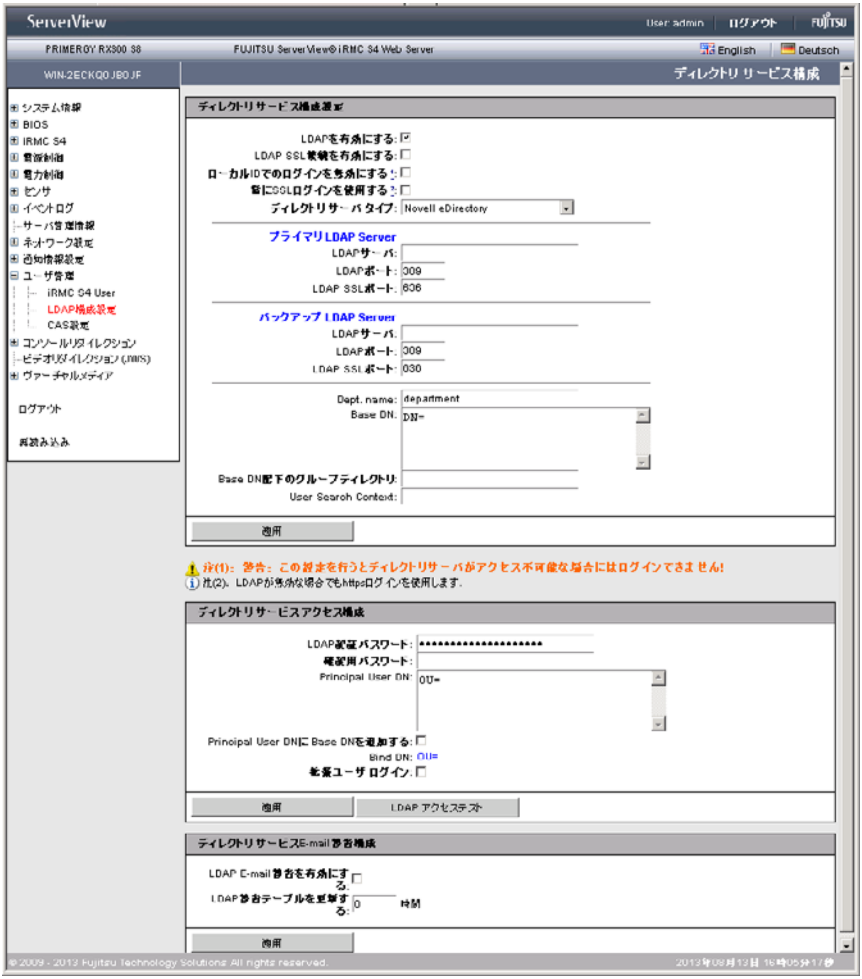


図 160: 「ディレクトリ サービス構成」ページ：Novell eDirectory/Open LDAP の仕様
Open LDAP

次の手順に従います。

▶ 「*ディレクトリサービス構成設定*」グループの設定を完成させます。

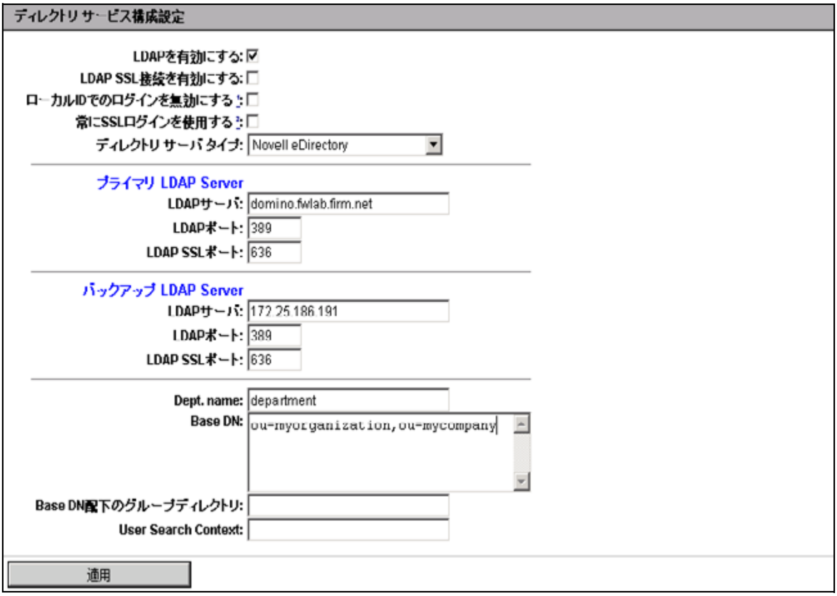


図 161:「ディレクトリ サービス構成」ページ - ディレクトリサービス構成設定 : Novell eDirectory/Open LDAP/OpenDS/Open DJ の仕様

プライマリ LDAP Server

使用する LDAP ディレクトリサーバ。

LDAP サーバ

プライマリ LDAP サーバの IP アドレスまたは DSN 名。

LDAP ポート

プライマリ LDAP サーバの LDAP ポート。

LDAP SSL ポート

プライマリ LDAP サーバのセキュアな LDAP ポート。

バックアップ LDAP Server

バックアップサーバとして運用され、「*LDAP サーバ 1*」が故障した場合のディレクトリサーバとして使用される LDAP ディレクトリサーバ。

LDAP サーバ

バックアップ LDAP サーバの IP アドレスまたは DSN 名。

LDAP ポート

バックアップ LDAP サーバの LDAP ポート。

LDAP SSL ポート

バックアップ LDAP サーバのセキュアな LDAP ポート。

Dept. name

部署名。ディレクトリサービスではユーザ許可を確認するときに部署名が必要です。Department X サーバと Department Y サーバでは、許可が異なることがあります。

Base DN

「*Base DN*」は、eDirectory または Open LDAP サーバの完全な分類名を示し、OU（組織単位）*の SVS* または *iRMCgroups* を含むツリーまたはサブツリーを表します。この DN は、LDAP 検索の開始点を示します。

Base DN 配下のグループディレクトリ

Base DN（Group DN Context）のサブツリーとして *SVS* または *iRMCgroups* を含む OU のパス名。

User Search Context

Base DN（User Search Context）のサブツリーとして OU（組織単位）*の Users* を含む OU のパス名。

► 「*適用*」をクリックすると設定が有効になります。

► 「*ディレクトリサービスアクセス構成*」グループで、LDAP アクセスデータを設定します。

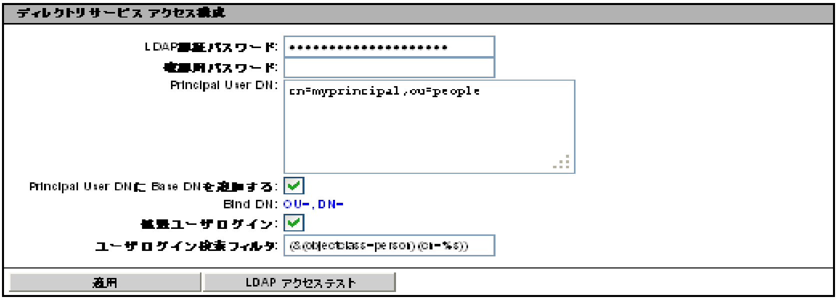


図 162: 「ディレクトリ サービス構成」ページ - ディレクトリサービスアクセス構成 : Novell eDirectory/Open LDAP

LDAP 認証パスワード

「*Principal User*」のパスワードを入力して LDAP サーバでの認証を行います。

パスワード確認

「*LDAP 認証パスワード*」に入力したパスワードをもう一度入力します。

Principal User DN

完全な構成名。iRMC S4 で作成されたユーザ ID（プリンシパルユーザ）の オブジェクトパスと属性の完全な記述で、これを使用して iRMC S4 は、LDAP サーバ からの iRMC S4 ユーザの許可を の問い合わせます。

Principal User DN に Base DN を追加する

このオプションが有効な場合、「*Principal User DN*」を設定する必要はありません。この場合、「*ディレクトリサービス構成設定*」グループの「*Base DN*」で設定した Base DN が使用されます。

Bind DN

「*Bind DN*」には、LDAP 認証で使用されるプリンシパルユーザ DN が表示されます。

拡張ユーザログイン

ユーザがログインする際の柔軟性を拡張します。

注意！

このオプションの有効化は、LDAP 構文に詳しい方のみご利用ください。不正な検索フィルタを設定して有効にすると「*拡張ユーザログイン*」オプションが無効になるまで、グローバルログインでの iRMC S4 へのログインができません。

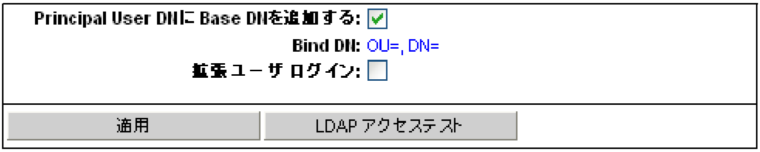


図 163: 拡張ユーザログイン

「*拡張ユーザログイン*」を選択して「*適用*」で有効にした場合、「*ユーザログイン検索フィルタ*」フィールドが追加で表示され、標準の検索フィルタ "(&(objectclass=person)(cn=%s))" が表示されます。

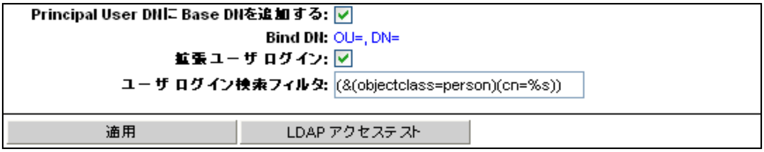


図 164: 「拡張ユーザログイン」用 LDAP 検索フィルタ

ログイン時に、プレースホルダ「%s」は対応するグローバルログインに置き換えられます。「cn=」の代わりに別の属性を指定することで、標準フィルタを変更することができます。すべてのグローバルログインが許可され、この検索フィルタの条件を満たす iRMC S4 へログインします。

LDAP アクセステスト

LDAP ディレクトリサーバへのアクセスデータをチェックし、LDAP の状態をその結果として表示します（図 158 を参照）。

> **i** このテストは基本的なアクセスデータ（「LDAP サーバが存在するか」あるいは 「ユーザは設定されているか」）を確認するもので、ユーザ認証のすべてを確認するものではありません。

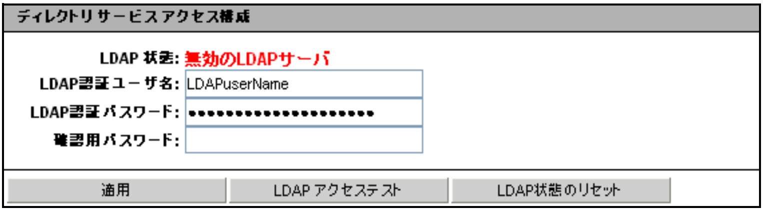


図 165: 「ディレクトリ サービス構成」ページ - LDAP サーバへの接続状況：Novell eDirectory/OpenLDAP

- 「*LDAP 状態のリセット*」ボタンをクリックして、画面への表示をリセットします。

- 「*適用*」をクリックすると設定が有効になります。

- 「*ディレクトリサービス E-mail 警告構成*」グループを使用して、グローバル Email 警告の設定を行います。

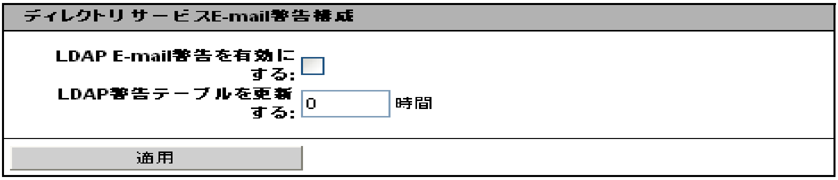


図 166: 「ディレクトリ サービス構成」ページ - ディレクトリサービス E-mail 警告構成

LDAP Email 警告を有効にする

グローバル Email 通知を有効にします。

LDAP 警告テーブルを更新する（時間）

Email テーブルを定期的に更新する間隔を定義します（『ServerView でのユーザ管理』を参照）。「0」を設定すると、テーブルは定期的に更新されなくなります。

- 「*適用*」をクリックすると設定が有効になります。

7.15.3 Centralized Authentication Service（CAS）設定 - CAS サービスの設定

このビューは、iRMC S4 が搭載される一部の PRIMERGY サーバではサポートされていません。

SSO は、Web インターフェースを使用して iRMC S4 にアクセスする場合のみサポートされます。SSO は、リモートマネージャ（Telnet/SSH）を使用して iRMC S4 にアクセスする場合は**サポートされません**。

「*Centralized Authentication Service（CAS）設定*」ページでは、CAS ベースのシングルサインオン（SSO）認証用の iRMC S4 Web インターフェースを設定できます。

CAS サービスの SSO ドメイン内のアプリケーションに初めてログインすると、CAS 固有のログイン画面でログイン認証情報の入力が要求されます。CAS サービスによる認証に成功すると、ユーザはログイン認証情報を再び入力せずに、iRMC S4 Web インターフェースと SSO ドメイン内の他のサービスへのアクセスが許可されます。

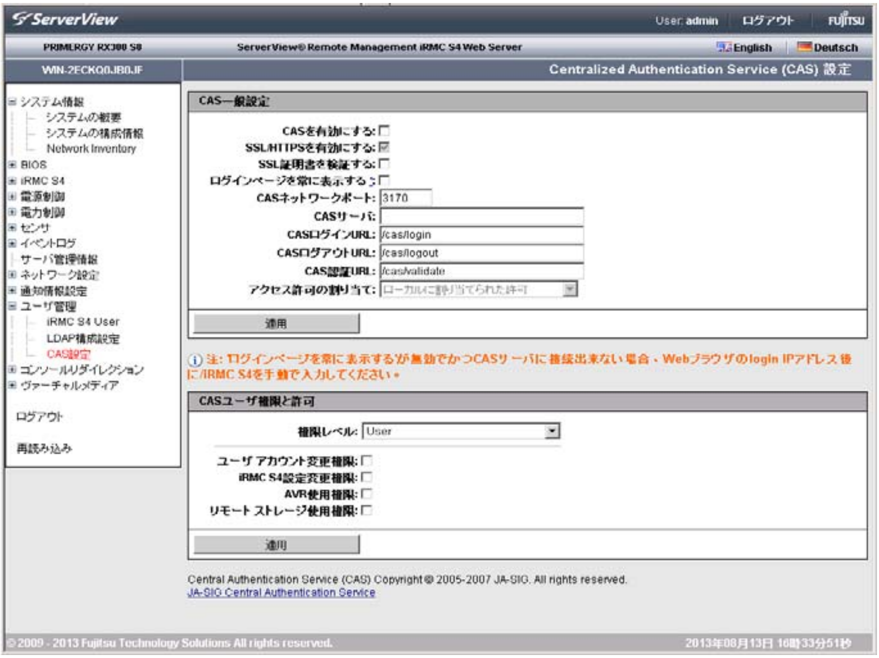


図 167: Centralized Authentication Service（CAS）設定

CAS 一般設定

「*CAS 一般設定*」グループでは、CAS アクセスデータを設定できます。

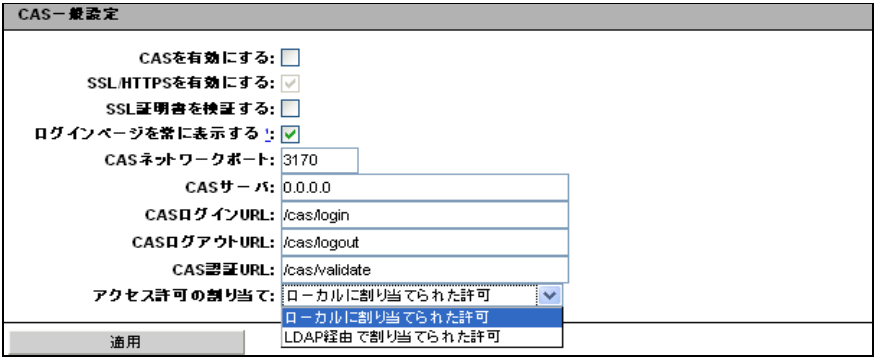


図 168: 「Centralized Authentication Service（CAS）設定」ページ - CAS 一般設定

CAS を有効にする

「*CAS 一般設定*」グループで指定する CAS サービスを使用して SSO を有効にします。

SSL/HTTPS を有効にする

CAS サービスと iRMC S4 間のすべての通信は SSL 暗号化されています。

SSL 証明書を検証する

CAS サービスの SSL 証明書を CA 証明書と照らし合わせて確認します。

ログインページを常に表示する

> **i** 「*ログインページを常に表示する*」が無効で CAS サービスにアクセスできない場合は、ブラウザのナビゲーションバーで、iRMC S4 の IP アドレスの後に /login と入力します。

iRMC S4 ログインページは常に表示されます。

図 169: ログインページ

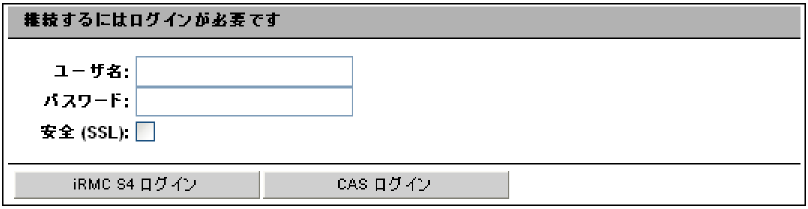


図 170: ログインページ - 明示的な認証情報の要求

これにより、「*CAS ユーザ権限と許可*」で定義した認証プロファイルとは異なる権限と許可を使用して、一時的に iRMC S4 にログインできます（281 ページを参照）。

たとえば、現在 CAS サービスに「*User*」権限を持つユーザ ID でログインしているときに、「*Administrator*」権限が必要な操作を行いたいとします。ユーザは、必要な権限を持つユーザ ID で一時的に iRMC S4 にログインできます。ただし、両方のユーザ ID 間で切り替えを行うことはできません。

「*iRMC S4 ログイン*」および「*CAS ログイン*」ボタンには次の機能があります。

iRMC S4 Login

「*ユーザ名*」と「*パスワード*」に指定した値を使用して、iRMC S4 Web インターフェースにログインします。CAS サービスはバイパスされます。

CAS ログイン

SSO を使用して iRMC S4 Web インターフェースにログインします。

– ユーザが CAS サービスによってまだ認証されていない場合：
  ユーザが CAS サービスによってまだ認証されていない場合、「*ユーザ名*」と「*パスワード*」に指定した値を使用して認証のために CAS サービスにリダイレクトされます。

– ユーザが CAS サービスによって既に認証されている場合：
  ユーザが CAS サービスによって既に認証されている場合、ユーザ名とパスワードの入力を要求されずに、iRMC S4 にログインします。

CAS ネットワークポート

CAS サービスの ポート。
デフォルトポート番号： 3170

CAS サーバ

CAS サービスの DNS 名。

i SSO ドメインに参加するすべてのシステムは、必ず同じアドレス表記を使用して中央管理用サーバ（CMS）を参照する必要があります。SSO ドメインは、同じ CAS サービスを使用して認証を行うすべてのシステムで構成されます。そのため、たとえば「my-cms.my-domain」という名前を使用して ServerView Operations Manager をインストールした場合、これとまったく同じ名前を使用して iRMC S4 の CAS サービスを指定します。そうせずに、「my-cms」のみや my-cms の別の IP アドレスを指定しても、SOS は 2 つのシステム間で有効になりません。

CAS ログイン URL

CAS サービスのログイン URL。

CAS ログアウト URL

CAS サービスのログアウト URL。

CAS 認証 URL

CAS サービスの URL を有効にします。

アクセス許可の割り当て

SSO を使用して iRMC S4 にログインするユーザの iRMC S4 権限と許可を定義します。

ローカルに割り当てられた許可
「*CAS User Privileg and Permissions*」で定義した権限と許可がユーザに適用されます。

LDAP 経由で割り当てられた許可
LDAP ディレクトリサービスで定義した認証プロファイルがユーザに適用されます。

i 「*LDAP 経由で割り当てられた許可*」オプションは、LDAP が有効な場合のみ使用できます（オプション 263 ページ の「LDAP を有効にする」を参照）。

CAS ユーザ権限と許可

「*CAS ユーザ権限と許可*」グループでは、ユーザが SSO を使用して iRMC S4 にログインする場合に、ユーザに許可する iRMC S4 権限と許可を定義できます。

i 「*CAS ユーザ権限と許可*」グループは、「*CAS 一般設定*」グループの「*アクセス許可の割り当て*」で「*LDAP 経由で割り当てられた許可*」が選択されている場合は表示されません。

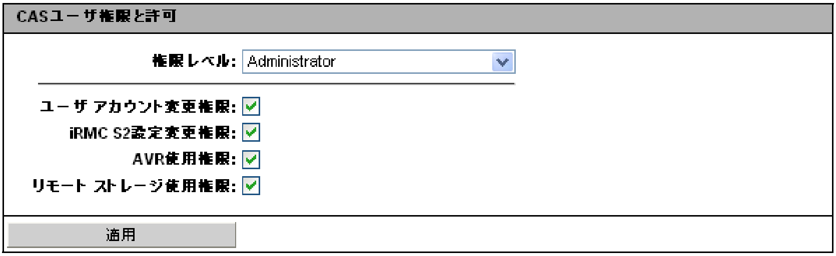


図 171: 「Centralized Authentication Service（CAS）設定」ページ - CAS ユーザ権限と許可

権限レベル
権限グループをユーザに割り当てます。

– *User*
– *Operator*
– *Administrator*
– *OEM*

権限グループに関連する許可に関する情報は、58 ページ の「ユーザ権限」の項 を参照してください。

IPMI 別許可に加えて、次のチャネル非依存許可を個別にユーザに割り当てることもできます。

ユーザアカウント変更権限
ローカルユーザアクセスデータを設定する権限。

iRMC S4 設定変更権限
iRMC S4 設定を行う権限。

AVR 使用権限
「View Only」および「フルコントロール」モードで AVR（ビデオリダイレクション）を使用する権限。

リモートストレージ使用権限
仮想メディア機能を使用する権限。

7.16 コンソールリダイレクション - コンソールのリダイレクト

次のページをコンソールリダイレクションに使用できます。

- 283 ページ の「BIOS テキストコンソール - テキストコンソールリダイレクションの設定と開始」
- 288 ページ の「ビデオリダイレクション（AVR）- ビデオリダイレクション（AVR）の開始」

7.16.1 BIOS テキストコンソール - テキストコンソールリダイレクションの設定と開始

「*BIOS テキストコンソール*」ページを使用して、テキストコンソールのリダイレクションの設定と開始ができます。

> **i** テキストコンソールのリダイレクションは、BIOS でも設定できます（45 ページ の「iRMC S4 のテキストコンソールリダイレクションの設定」の項を参照）。

図 172: 「BIOS テキストコンソール」ページ

7.16.1.1 BIOS コンソールリダイレクションオプション - テキストコンソールリダイレクションの設定

*「BIOS コンソールリダイレクションオプション」*を使用して、テキストコンソールのリダイレクションを設定できます。

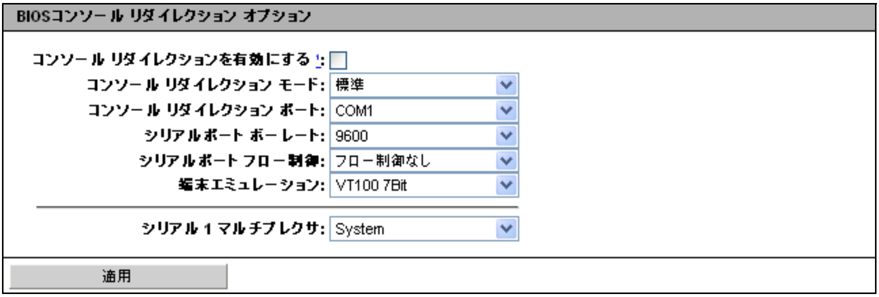


図 173: 「BIOS テキストコンソール」ページ - BIOS コンソールリダイレクションオプション

コンソールリダイレクションを有効にする

このオプションで、コンソールリダイレクションを有効 / 無効にできます。

> **i** オペレーティングシステムでも、BIOS 設定にかかわらず、テキストコンソールのリダイレクションを許可することができます。

シリアルポート ボーレート

次のボーレートが設定可能です : 9600、19200、38400、57600、115200。

シリアルポートフロー制御

次の設定が可能です。

なし

フロー制御を行いません。

XON/XOFF（Software）

通信制御がソフトウェアによって行われます。

CTS/RTS（Hardware）

通信制御がハードウェアによって行われます。

端末エミュレーション

次の端末エミュレーションを使用できます。

VT100 7Bit、*VT100 8Bit*、*PC-ANSI 7Bit*、*PC-ANSI 8 Bit*、*VT100+*、*VT-UTF8*

シリアル 1 マルチプレクサ

マルチプレクサの設定との整合性を確認します。

– Serial：システム
– LAN：iRMC S4

► 「*適用*」をクリックすると設定が有効になります。

7.16.1.2 オペレーティングシステム実行中のテキストコンソールのリダイレクション

管理対象サーバのオペレーティングシステムによっては、BIOS POST フェーズ後もコンソールリダイレクションの使用を継続することができます。

DOS

> 条件：
>
> コンソールリダイレクションの BIOS 設定が、「*Enhanced*」に設定されている必要があります（283 ページ の「BIOS テキストコンソール - テキストコンソールリダイレクションの設定と開始」を参照）。

管理対象サーバで PRIMERGY ServerView Suite 診断ソフトウェアを起動する場合は、コンソールリダイレクションを使用して、PRIMERGY ServerView Suite 診断を操作することができます。

Windows Server 2008/2012

Windows Server 2008/2012 では、POST フェーズ後、自動的にコンソールリダイレクションを使用できます。さらに設定を行う必要はありません。オペレーティングシステムの起動中に、Windows Server 2008 SAC コンソール /Windows Server 2012 SAC コンソールに切り替わります。

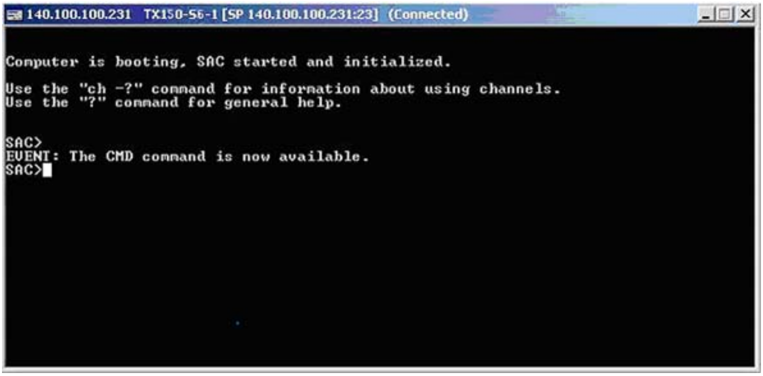


図 174: Windows Server SAC コンソール

Linux

Linux オペレーティングシステムでは、POST フェーズ後にコンソールリダイレクションを使用するために、次の設定を行う必要があります。一度設定すると、リモートアクセスも可能になります。

必要な設定

設定は、プログラムのバージョンによって異なる場合があります。

SuSe および RedHat

/etc/inittab ファイルの最後に次の行を追加します。

xx:12345:respawn:/sbin/agetty <baud-rate> ttyS0

RedHat

/etc/grub.conf ファイルのカーネルブートパラメータに以下を追加します。

console=ttyS0,<baud-rate> console=tty0

SuSE

/boot/grub/menu.lst ファイルのカーネルブートパラメータに以下を追加します。

console=ttyS0,<baud-rate> console=tty0

7.16.2 ビデオリダイレクション（AVR）- ビデオリダイレクション（AVR）の開始

「*ビデオリダイレクション（AVR）*」ページを使用して、グラフィカルなコンソールリダイレクションを開始できます。「ビデオリダイレクション」機能では、管理対象サーバからのグラフィカルな出力をリモートワークステーションにリダイレクトし、リモートワークステーションのキーボードおよびマウス入力を管理対象サーバに割り当てるので、ローカルで作業しているかのようにリモートワークステーションから管理対象サーバにアクセスできます。

AVR は、同時に 2 人のユーザが使用できます。一方のユーザがサーバをフルコントロールしている場合（フルコントロールモード）、もう一方のユーザは、キーボードおよびマウスの操作を表示するだけしかできません（ビューモード）。

i iRMC S4 の「*ビデオリダイレクション（AVR）*」ファンクションを使用するには、ライセンスキーが必要です（159 ページ の「「iRMC S4 情報」- iRMC S4 上の情報」の項を参照）。

AVR 機能には、Java アプレットが使用されています。

i **注意事項：**

Java キャッシングを**無効にしないでください**。無効にすると AVR を起動できません。（デフォルトでは Java キャッシングは有効です）。

図 175: 「ビデオリダイレクション（AVR)」ページ

AVR 実行中セッション - 現在の AVR セッションの表示

「*AVR 実行中セッション表*」には、現在の実行中の AVR セッションが表示されます。AVR セッションが実行されていない場合、「*AVR 実行中セッション表*」は表示されません。

2 つの AVR セッションが現在実行されている場合、「*Disconnect*」ボタンが各セッションに表示されます。

AVR実行中セッション表

番号	IPアドレス	ユーザ名	ユーザID	アクセス権限	ストレージ有効	コントロール取得可能	セッション状況	
1	172.25.51.40	admin	2	フルコントロール	Yes	Yes	確立済	切断
2	217.9.101.18	admin	2	表示のみ	No	Yes	確立済	切断

図 176: AVR 実行中セッション - （2 つの AVR セッションが実行中の場合）

切断

「*切断*」ボタンをクリックすると、確認ダイアログが表示され、左側のボタンで、AVR セッションを閉じることができます。

i 「*切断*」ボタンを使用してのみ、他のユーザの AVR セッションを閉じることができます。ユーザ固有のセッションを閉じるには、「*拡張機能*」メニューか ら、「*Exit*」ボタンを使用します（87 ページを参照）。

ビデオリダイレクション

> **i** この機能は、一部の PRIMERGY サーバでサポートされていません。

「*ビデオリダイレクション*」グループでは、AVR セッション中に適用される各種オプションを指定できます。

図 177: 「ビデオリダイレクション (AVR)」ページ - ビデオリダイレクションオプション

既定のマウスモード

デフォルトマウスモード（「*Absolute Mouse Mode*」、「*Relative Mouse Mode*」、「*Other Mouse Mode*」）を定義します。

サーバの OS に応じて、以下の設定を指定する必要があります。

- Windows :「*Absolute mouse mode*」、「*Hide mouse mode (Relative)*」、「*Relative mouse mode*」のいずれか。
- Linux :「*Absolute mouse mode*」、「*Hide mouse mode (Relative)*」、「*Relative mouse mode*」のいずれか。

> **i** デフォルト設定 :「*Absolute mouse mode*」。

ビデオリダイレクション中は USB ポートを無効化する

AVR セッション中に管理対象サーバで無効にする USB ポートを定義します。

なし

どの USB ポートも無効になりません。

全面 USB コネクタ

サーバの前面の USB ポートのみが使用不可能になります。

背面 USB コネクタ

サーバの背面の USB ポートのみが使用不可能になります。

すべて無効

サーバのすべての USB ポートが無効になります。

サーバ側モニタの表示オフ制御

i サーバ側モニタの現在のステータスは AVR の「*Video*」メニューに示され、AVR ツールバーの右から 2 番目のアイコンを使用して表示されます（105 ページ の「AVR ツールバー」の項を参照）。

iRMC S4 の「*Local Monitor Off Control*」機能を有効 / 無効にします。

有効

「*Local Monitor Off Control*」機能を有効にします。AVR セッションのフルアクセスモードでは、サーバのサーバ側モニタのオン / オフをリモートワークステーションから切り替えることができます。

無効

「*Local Monitor Off Control*」機能を無効にします。つまり、サーバ側モニタは常にオンになり、オフに切り換えることはできません。

AVR 開始時の自動オフ

i このオプションは、「*サーバ側モニタの表示オフ制御*」機能が有効な場合のみ有効です。

「*AVR 開始時の自動オフ*」オプションを有効にした場合、サーバ側モニタの電源は、AVR セッションが開始されるとセッション中に自動的にオフになります。「*サーバ側モニタの表示オフ制御*」が有効な同時セッションがない場合、AVR セッションが終了すると、サーバ側モニタの電源が再び自動的にオンになります。

i **同時 AVR セッション**：

AVR セッション中にサーバ側モニタの電源をオンにしても、新しい同時 AVR セッションが開始されると、サーバ側モニタの電源は再び自動的にオフになります。

サーバ側モニタの電源は、AVR セッションが終了すると自動的にオンになります。

AVR タイトル

AVR タイトルバーに表示するタイトルを選択します。

> i AVR タイトルには以下の事前に定義された変数を使用できます。
>
> %USER%, %BMC,_NAME%, %BMC_IP%, %CHASSIS_TYPE%, %SYSTEM_TYPE%, %SYSTEM_SERIAL%, %SYSTEM_NAME%, %SYSTEM_IP%, %SYSTEM_OS%, %ASSET_TAG%

現在の AVR タイトル

AVR タイトルバーに表示する AVR タイトルバーを表示します。

► 「*適用*」をクリックすると設定が有効になります。

ビデオリダイレクション - AVR の開始

「*ビデオリダイレクションの開始*」を使用して AVR を開始します。

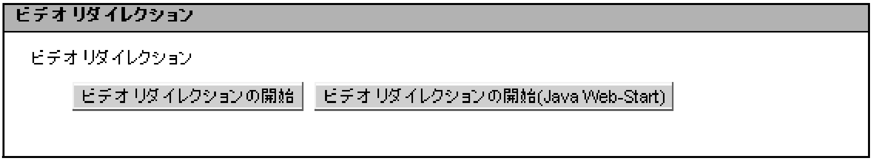


図 178: 「ビデオリダイレクション（AVR）」ページ - サーバ側のモニタ

▶ 「*ビデオリダイレクションの開始（Java Web-Start）*」をクリックして、2 番目の AVR セッションを開始します。

ビデオリダイレクションのための Java アプレットが開始されます。

> **i** AVR ウィンドウの詳細については、75 ページ の「ビデオリダイレクション（AVR）」の章を参照してください。

2 つの有効な AVR セッションは、「*ビデオリダイレクション（AVR）*」ページで次のように表示されます。

図 179: 2 つの AVR セッションが有効な場合の AVR 画面

切断

「*切断*」ボタンをクリックすると、確認ダイアログが表示され、左側のボタンで、AVR セッションを閉じることができます。

> 「*切断*」ボタンを使用してのみ、他のユーザの AVR セッションを閉じることができます。ユーザ固有のセッションを閉じるには、「*拡張機能*」メニューか ら、「*Exit*」ボタンを使用します（87 ページを参照）。

管理サーバの電源がオフの場合は次の画面が表示されます。

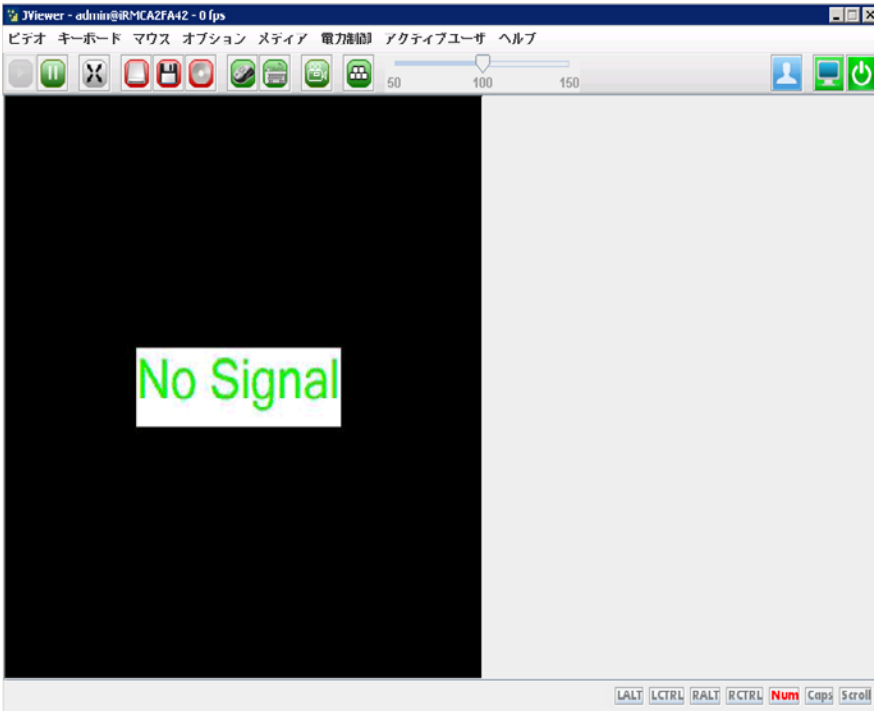


図 180: 管理サーバの電源がオフの場合の AVR 画面

7.17 ヴァーチャルメディア

仮想メディア機能によって、物理的にネットワーク内の任意の場所に存在できる、仮想ドライブ（フロッピードライブまたは CD ROM）を管理対象サーバで使用できるようになります。仮想ドライブとして、物理ドライブ（フロッピーディスクドライブあるいは CD-ROM/DVD-ROM）あるいは ISO イメージ（イメージファイル）を使用することができます。

i iRMC S4 の*仮想メディア*機能を使用するには、ライセンスキー（161 ページを参照）が必要です。

仮想メディアは、リモートワークステーションで物理ドライブまたはイメージファイルとして使用可能にできます（110 ページを参照）。イメージファイルはネットワークドライブ（たとえば、D ドライブの場合「D:」ドライブ文字を使用）でも構いません。

「*Virtual Media link*」には、次のページへのリンクが含まれます。

– 297 ページ の「「ヴァーチャルメディアオプション」- 仮想メディアオプションの設定」

– 299 ページ の「「リモートイメージマウント」- リモート ISO イメージへの接続」

i このリンクが表示されるのは、「*リモートイメージマウント*」のサポートが「*ヴァーチャルメディアオプション*」ページで有効になっている場合のみです。

7.17.1 「ヴァーチャルメディアオプション」- 仮想メディアオプションの設定

「*ヴァーチャルメディアオプション*」ページでは、iRMC S4 によって提供される仮想メディアのオプションを設定できます。

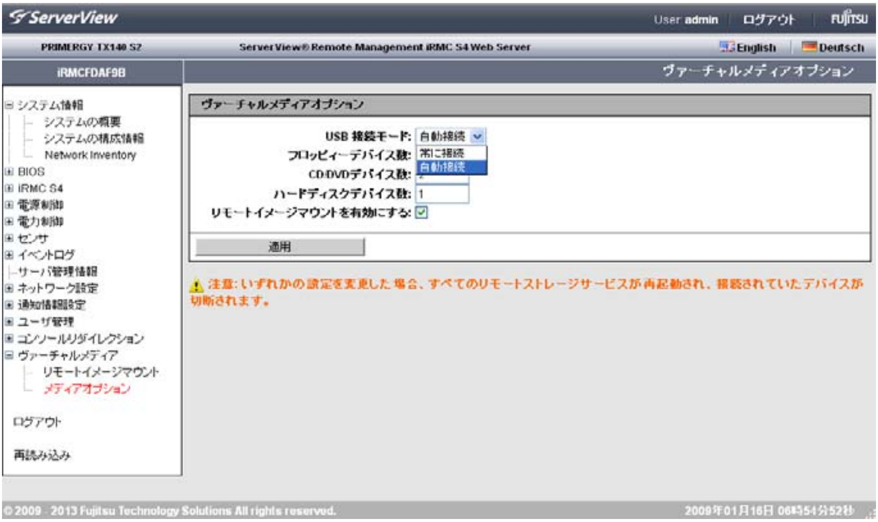


図 181: 「ヴァーチャルメディアオプション」ページ

USB 接続モード

仮想メディアの接続モード。

以下のモードを選択できます。

常に接続

仮想メディアは常にサーバに接続されます。

自動接続

仮想メディアセッションが開始されているときのみ、仮想メディアはサーバに接続されます。

フロッピィーデバイス数

仮想メディアセッションで使用可能なフロッピーデバイスの最大数。0 ～ 4 台のフロッピーデバイスを設定できます。

CD/DVD デバイス数

仮想メディアセッションで使用可能な CD/DVD デバイスの最大数。0 ～ 4 台の CD/DVD デバイスを設定できます。

ハードディスクデバイス数

仮想メディアセッションで使用可能なハードディスクデバイスの最大数。0 ～ 4 台のハードディスクデバイスを設定できます。

リモートイメージマウントを有効にする

CD/DVD、フロッピー、ハードディスク ISO イメージをネットワークのサーバでホストできるようにする、リモートイメージマウントを有効 / 無効にします。

「リモートイメージマウントを有効にする」オプションをアクティブにすると、ナビゲーション領域の「*ヴァーチャルメディア*」に「*リモートイメージマウント*」リンクが表示されます。「*リモートイメージマウント*」リンクをクリックすると、「*イメージオプション*」を設定するパネルのある「*リモートイメージマウント*」ページが開きます（299 ページを参照）。

► 「*適用*」をクリックすると設定が有効になります。

7.17.2 「リモートイメージマウント」- リモート ISO イメージへの接続

リモートイメージマウント機能により、管理対象サーバで、ネットワークのサーバでホストされる CD/DVD、フロッピー、ハードディスク ISO イメージを使用できるようにします。

「*リモートイメージマウント*」ページには、対応するイメージタイプ（CD/DVD、フロッピー、ハードディスク ISO イメージ）の「*イメージオプション*」を設定するためのグループが含まれます。

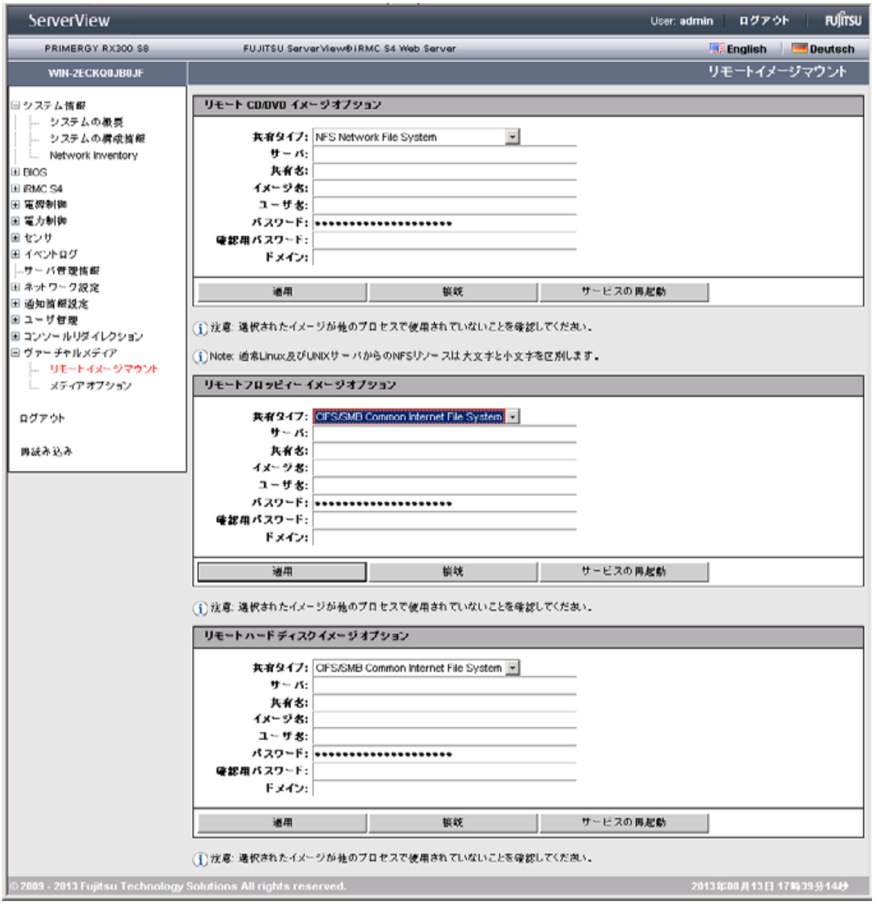


図 182: 「リモートイメージマウント」ページ

リモート CD/DVD イメージオプション / リモートフロッピィーイメージオプション / リモートハードディスクイメージオプション

これらの各グループでは、対応するタイプのリモートイメージをマウントするオプションの設定、およびリモートイメージへの接続の確率 / クリアができます。また、「*リモートイメージマウント*」サービスを再起動することもできます（障害の場合など）。

共有タイプ

ISO イメージが保存されているネットワーク共有の共有タイプ。

以下のモードを選択できます。

CIFS/SMB Common Interface File System

ネットワーク共有の共有タイプが CIFS SMB（Common Interface File System）。

NFS Network File System

仮想メディアセッションが開始されているときのみ、仮想メディアはサーバに接続されます。

サーバ

リモートイメージをホストするサーバ（略してリモートイメージサーバ）の IP アドレスまたは DNS 名。

共有名

リモートイメージサーバが属するネットワーク共有の名前。

イメージ名

リモートイメージの名前 / リモートイメージへのパス。

ユーザ名

ネットワーク共有にアクセスするために必要なユーザ名。

パスワード

ユーザのパスワードを入力します。

確認用パスワード

確認のために、パスワードを再入力します。

ドメイン

ユーザのドメイン。

適用

設定をアクティブにします。

接続

リモートイメージを管理対象サーバに接続します。

切断

リモートイメージの接続をクリアします。

サービスの再起動

「リモートイメージマウント」サービスを再起動します（障害の場合など）。

リモートイメージの管理対象サーバへの接続

「*リモート CD/DVD イメージオプション*」を次のように設定した場合：

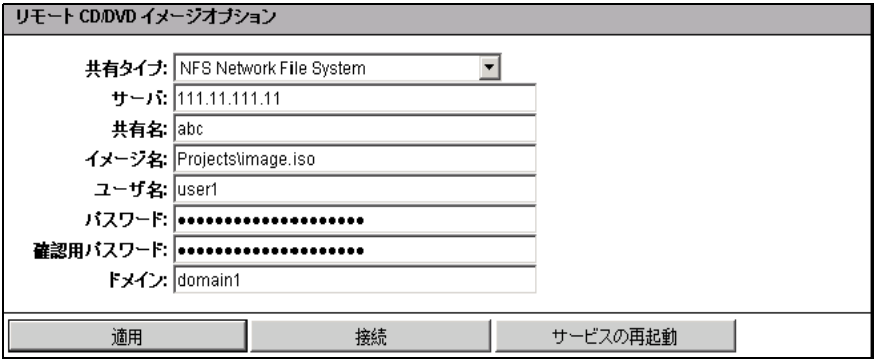


図 183: 「リモート CD/DVD イメージオプション」が設定されている

リモートイメージを管理対象サーバに接続するには、次の手順に従います。

- ►「*適用*」をクリックすると設定が有効になります。
- ►「*接続*」をクリックします。

  「*リモート CD/DVD イメージオプション*」グループが次のように表示され、現在リモートイメージが管理対象サーバに接続されていることを示します。

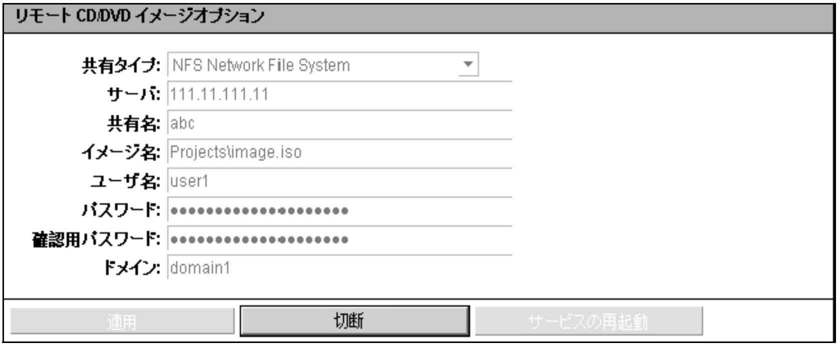


図 184: 「リモート CD/DVD イメージオプション」

► リモートイメージへの接続をクリアするには、「*切断*」をクリックします。

► 「*リモートイメージマウント*」サービスを再起動するには（障害の場合など）、「*サービスの再起動*」をクリックします。

8 Telnet/SSH 経由の iRMC S4 (リモートマネージャ)

iRMC S4 では Telnet ベースのインターフェースを使用できます。このインターフェースはリモートマネージャと呼ばれています。リモートマネージャは、Telnet/SSH クライアント経由で呼び出すことができます。

iRMC S4 は SSH（**S**ecure **Sh**ell）によるセキュア接続をサポートします。リモートマネージャインターフェースは Telnet および SSH 接続と同じものです。原則として、VT100 シーケンスを解釈する Telnet/SSH クライアントであれば、iRMC S4 へのアクセスに使用できます。ただし、iRMC S4 Web インターフェースまたは ServerView Remote Management Frontend（以下では単に Remote Management Frontend と呼ぶ）の使用を推奨します。

i 同時セッションの最大数：

– Telnet：最大 4
– SSH：最大 4
– Telnet および SSH の合計：最大 4

この章では、リモートマネージャからの iRMC S4 の操作および各種機能の詳細を説明します。末尾には、SMASH CLP の概要も示します。

8.1 管理対象サーバに関する要求

Telnet を使用する iRMC S4 へのアクセスを有効にする必要があります（237 ページ の「ポート番号とネットワークサービス - ポートとネットワークサービスの設定」を参照）。

> **i** パスワードはプレーンテキストで送信されるので、Telnet プロトコルを使用したアクセスはデフォルトでは無効です。

> **i** ServerView Operations Manager にはマネジメントポートの価値が認識されないため、Remote Management Frontend はデフォルト値で動作します。
>
> Remote Management Frontend が起動したときに自動的に接続は確立されないので、Remote Management Frontend が起動した後にマネジメントポートの標準以外の値を変更できます。

8.2 リモートマネージャの操作

リモートビューの操作を図 185 の例に基づいて説明します。この図では、リモートマネージャのメインメニューの一部を示しています。

```
    Main Menu

(1) System Information...
(2) Power Management...
(3) Enclosure Information...
(4) Service Processor...
(5) RAID Management...

(c) Change password
(r) Console Redirection (EMS/SAC)
(s) Start a Command Line shell...
(l) Console Logging

Enter selection or (0) to quit:
```

図 185: リモートマネージャの操作

- メニュー項目の先頭の文字または数字を入力して、必要なメニューを選択します。たとえば、「パスワードの変更（Change password）」の場合は「c」と入力します。

  ユーザが使用を許されていないファンクションはダッシュ (-) で、また提供されていないファンクションはアステリスク (*) で指示してあります。

- [0] または [Ctrl]+[D] キー押して、リモートマネージャを閉じます。適切なイベントがイベントログに書き込まれます。

8.3 メニューの概要

iRMC S4 のリモートマネージャのメニューは、次の構造になっています。

- **システム情報**
  - 「View Chassis Information」
  - 「View Mainboard Information」
  - 「View OS and SNMP Information」
  - Set ASSET Tag
- **電源制御**
  - 電源切断
  - ハードリセット
  - 電源 Off-On
  - 電源投入
  - 電源切断（シャットダウン）
  - リセット（シャットダウン）
  - Raise NMI（via iRMC S4）
- **外装情報**
  - システムイベントログ
    - View System Eventlog (text, newest first)(システムイベントログの表示 (テキスト、新しいものから))
    - View System Eventlog (text, oldest first)
    - Dump System Eventlog (raw, newest first) (イベントログのダンプ (画像、新しいものから))
    - Dump System Eventlog (raw, oldest first) (イベントログのダンプ (画像、古いものから))
    - システムイベントログ情報の表示
    - Clear System Eventlog (システムイベントログの消去)

- Internal Eventlog
  - View Internal Eventlog (text, newest last)
  - Dump Internal Eventlog (raw, newest last)
  - View Internal Eventlog Information
  - Clear Internal Eventlog
  - Change Internal Eventlog mode
- 温度
- Voltages/Current
- ファン
- Power Supplies
- Memory Sensor
- Door Lock
- CPU Sensors
- Component Status (Lightpath)
- すべてのセンサのリスト

● **Service Processor**

- IP パラメータの設定
- List IP Parameters (IP パラメータのリスト)
- 識別灯のトグル
- Reset iRMC S4（Warm reset）
- Reset iRMC S4（Cold reset）

● **RAID Management**

- Controller information
- Physical device information
- Logical device information
- Array configuration information
- BBU status

- **Change password**
- **Console Redirection (EMS/SAC)**
- **コマンドラインシェルの起動**
- **Console Logging**

8.4 ログイン

iRMC S4 に接続する際、ログイン資格情報（ユーザ名とパスワード）の入力が必要です。iRMC S4 への接続が確立されるとすぐに、リモートマネージャのログインウィンドウ（Telnet/SSH ウィンドウ）がリモートワークステーションのターミナルクライアントに表示されます。

ServerView エージェントがある時点ですでにシステム上で起動しているかいないかで、ログインウィンドウの表示は、システム情報付きとシステム情報なしになります。

> **i** SSH 接続でログインした場合 : 管理対象サーバのホストキーがリモートワークステーションにまだ登録されていない場合、SSH クライアントはセキュリティ警告を発行し、推奨する続行方法を示します。

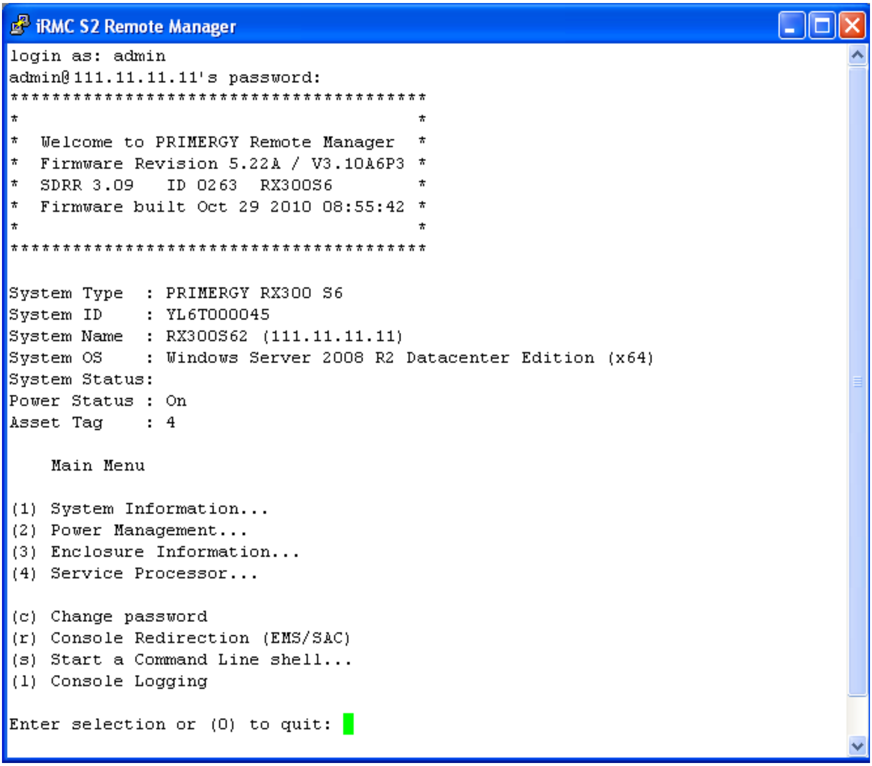


図 186: リモートマネージャ : メインメニューウィンドウ（システム情報付き）

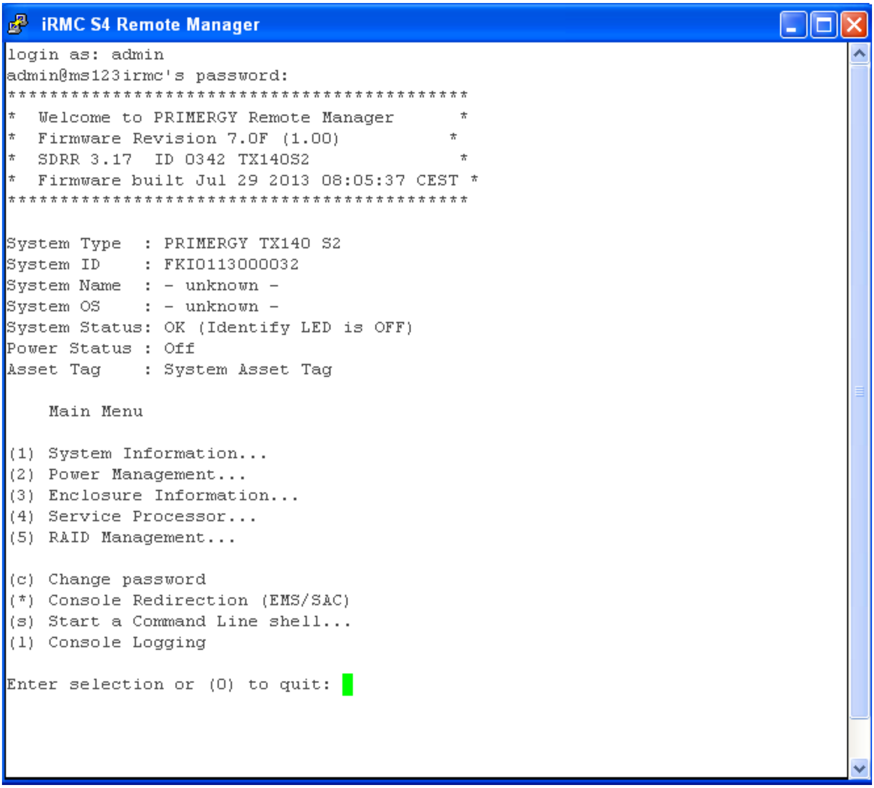


図 187: リモートマネージャ : メインメニューウィンドウ（システム情報なし）

リモートマネージャウィンドウには、影響を受けるシステムに関する情報が表示されます。その情報はサーバを識別し、その稼動状態 (電源状態) を表示します。サーバについてはいくつかの詳細情報 (システム名など) だけが、かつ、そのサーバが適切に設定されている場合に限り示されます。

▶ リモートマネージャが使用できるためには、ユーザ名とパスワードでログインしなければなりません。

次に、該当するイベントがイベントログに書き込まれ、リモートマネージャの関連のあるメインメニューが表示されます (311 ページ の「リモートマネージャのメインメニュー」の項 を参照してください)。

ログインプロセスは、[Ctrl] [D] を使用していつでも終了できます。

8.5 リモートマネージャのメインメニュー

```
    Main Menu

(1) System Information...
(2) Power Management...
(3) Enclosure Information...
(4) Service Processor...
(5) RAID Management...

(c) Change password
(r) Console Redirection (EMS/SAC)
(s) Start a Command Line shell...
(l) Console Logging

Enter selection or (0) to quit:
```

図 188: リモートマネージャ : メインメニュー

リモートマネージャのメインメニューには、次のファンクションが載っています。

「*System Information...*」	管理対象サーバの情報を表示し、資産タグを設定します (315 ページ の「システム情報 - 管理対象サーバの情報」の項を参照)。
Power Management...	サーバの電源をオン / オフします (317 ページ の「電源制御」の項を参照)。
「Enclosure Information...」	現在のシステム状態に関する情報を要求。たとえば、エラーログとイベントログからのエラーやイベントのメッセージ (温度、ファンなど) をチェックします。 (318 ページ の「Enclosure Information - システムイベントログとセンサの状態」の項を参照)。

表 9: リモートマネージャのメインメニュー

「Service Processor...」	iRMC S4 を設定します（ファームウェアの更新または IP アドレスの変更など） (323 ページ の「サービスプロセッサ - IP パラメータ、識別灯、iRMC S4 リセット」の項を参照)。
「RAID Managerment..」	RAID コントローラ、物理デバイス、論理デバイス、アレイ設定、BBU ステータスに関する情報 (324 ページ の「RAID Management」の項を参照)。
「Change password」	Change Password (315 ページ の「Change Password」の項を参照)。
「Console Redirection (EMS/SAC)」	テキストコンソールリダイレクション (325 ページ の「Console Redirection (EMS/SAC) - テキストコンソールリダイレクションの開始」の項を参照)。
「*Start a Command Line shell...*」	コマンドラインシェルの起動 (325 ページ の「コマンドラインシェルの起動 ...- SMASH CLP シェルの起動」の項を参照)。
Console Logging	メッセージ出力をテキストコンソールにリダイレクトします (326 ページ の「Console Logging - メッセージ出力のテキストコンソールへのリダイレクト（シリアル）」の項を参照)。

表 9: リモートマネージャのメインメニュー

8.6 必要なユーザ権限

表 10 に、リモートマネージャの個々の機能を使用するために必要なユーザ権限の概要を示します。

リモートマネージャのメニュー項目	IPMI レベルで許可				必要な許可			
	OEM	Administrator	Operator	ユーザ	ユーザアカウント変更権限	iRMC S4 設定変更権限	AVR 使用権限	リモートストレージ使用権限
View *System Information...*	X	X	X	X				
View Chassis / Mainboard / OS Information						X		
Set ASSET Tag1)						X		
Set System Name **1)**						X		
Set System Operating System Information**1)**						X		
Set System Description**1)**						X		
Set System Location Information（SNMP）1)						X		
Set System Contact Information (SNMP)**1)**						X		
Power Management...	X	X	X					
View *Enclosure Information*	X	X	X	X				
System Eventlog - View/Dump System Eventlog (システムイベントログ - システムイベントログの表示 / ダンプ)	X	X	X	X				
System Eventlog - Clear System Eventlog (システムイベントログ - システムイベントログの消去)	X	X	X					
Internal Eventlog - View/Dump Internal Eventlog	X	X	X	X				
Internal Eventlog - Clear Internal Eventlog	X	X	X	X				
Sensor overviews (温度 , ファン ...)	X	X	X	X				
View *Service Processor...*	X	X	X	X				

表 10: リモートマネージャのメニューを使う許可

リモートマネージャのメニュー項目	IPMI レベルで許可				必要な許可			
	OEM	Administrator	Operator	ユーザ	ユーザアカウント変更権限	iRMC S4 設定変更権限	AVR 使用権限	リモートストレージ使用権限
「Service Processor...」List IP Parameters (IP パラメータのリスト)						X		
「Service Processor...」List IP Parameters (IP パラメータのリスト)						X		
「Service Processor...」 - ID LED のトグル	X	X	X	X				
Service Proc....- Reset iRMC S4（warm/cold reset）	X	X						
View *RAID Management*.2)	X	X						
View Controller information2)	X	X						
View physical device information2)	X	X						
View logical device information2)	X	X						
View array configuration information2)	X	X						
View BBU status 2	X	X						
パスワードの変更					X			
「Console Redirection (EMS/SAC)」	X	X	X					
コマンドラインシェルの起動 ...	X	X	X	X				
Console Logging	X	X	X					

1) 実行中のエージェントがない場合のみの動作
2) システムによって異なる機能

表 10: リモートマネージャのメニューを使う許可

8.7 Change Password

「*Change password*」(パスワードの変更) メニュー項目から、「*ユーザ アカウント変更権限*」の特権を持つユーザ (58 ページ を参照) は、自分のパスワードや他のユーザのパスワードを変更することができます。

8.8 システム情報 - 管理対象サーバの情報

メインメニューから *System Information...* (システム情報) を選ぶと、次のメニューが現われます。

```
    System Information Menu

(1)  View Chassis Information
(2)  View Mainboard Information
(3)  View OS and SNMP Information

(4)  Set ASSET Tag
(*)  Set System Name
(*)  Set System Operating System Information
(*)  Set System Description
(*)  Set System Location Information (SNMP)
(*)  Set System Contact Information (SNMP)

Enter selection or (0) to quit:
```

図 189: リモートマネージャ : 「システム情報」メニュー

サブメニューには次のファンクションがあります。

「*View Chassis Information*」	管理対象サーバのシャーシと本番データの情報。
「*View Mainboard Information*」	管理対象サーバのメインボードと本番データの情報。
「*View OS and SNMP Information*」	管理対象サーバのオペレーティングシステムと ServerView バージョンの情報と、SNMP 設定の情報。

表 11: システム情報メニュー

Set ASSET Tag	管理対象サーバのカスタマ固有の資産タグを設定します。

表 11: システム情報メニュー

8.9 電源制御

メインメニューから「*Power Management...*」を選択すると、次のメニューが表示されます。

```
    Power Management Menu

(1) Immediate Power Off
(2) Immediate Reset
(3) Power Cycle
(*) Power On

(5) Graceful  Power Off (Shutdown)
(6) Graceful  Reset     (Reboot)
(n) Raise NMI (via iRMC S2)

Enter selection or (0) to quit:
```

図 190: リモートマネージャ : 「Power Management」メニュー

サブメニューには次のファンクションがあります。

電源切断	オペレーティングシステムの状態にかかわらず、サーバの電源を切断します。
ハードリセット	オペレーティングシステムの状態にかかわらず、サーバを完全に再起動します（コールドスタート）。
電源 Off-On	サーバの電源が完全に切断され、設定した時間の経過後、再び投入されます。
電源投入	サーバの電源を投入します。
電源切断（シャットダウン）	グレースフルシャットダウンし、電源を切断します。 このメニュー項目は、ServerView エージェントが iRMC S4 にインストールされ、「Connected」として署名されている場合にのみ使用できます。
リセット（シャットダウン）	正常にシャットダウンして、再起動します。 このメニュー項目は、ServerView エージェントが iRMC S4 にインストールされ、「Connected」として署名されている場合にのみ使用できます。

表 12: 「Power Management」メニュー

8.10 Enclosure Information - システムイベントログとセンサの状態

メインメニューから *Enclosure Information...* (外装情報) を選ぶと、次のメニューが現われます。

```
    Enclosure Information Menu

(e) System Eventlog
(i) Internal Eventlog
(t) Temperature
(v) Voltages/Current
(f) Fans
(p) Power Supplies
(d) Door Lock
(m) Memory Sensors
(c) CPU Sensors
(s) Component Status
(l) List All Sensors

Enter selection or (0) to quit:
```

図 191: リモートマネージャ : 「Enclosure Information」メニュー

サブメニューには次のファンクションがあります。

システムイベントログ	「*System Eventlog*」メニューを呼び出します（320 ページ の「システムイベントログ」の項を参照）。
Internal Eventlog	「*internal Eventlog*」メニューを呼び出します（322 ページ の「Internal Eventlog」の項を参照）。
温度	温度センサとその状態に関する情報を表示します。
Voltages/Current	電圧と電流センサ、およびその状態の情報を表示します。
ファン	ファンとセンサとその状態に関する情報を表示します。
Power Supplies	電源と冗長の状態の情報を表示します。
Door Lock	フロントパネルまたはハウジングが開いているかどうかを表示します。
Memory Sensors	メモリの状態に関する情報を表示します。
CPU Sensors	サーバのプロセッサの位置を特定します。
コンポーネントの状態	PRIMERGY 診断 LED をそなえたすべてのセンサに関する詳細な情報を表示します。
すべてのセンサのリスト	すべてのセンサの詳細な情報を表示します。

表 13: 外装情報メニュー

システムイベントログ

「*Enclosure Information...*」サブメニューから「*System Eventlog*」を選択すると、次のメニューが表示されます。

```
    System Eventlog Menu

(1) View System Eventlog (text, newest first)
(2) View System Eventlog (text, oldest first)
(3) Dump System Eventlog (raw, newest first)
(4) Dump System Eventlog (raw, oldest first)

(5) View System Eventlog Information
(6) Clear System Eventlog

Enter selection or (0) to quit:
```

図 192: リモートマネージャ : 「System Eventlog」メニュー

サブメニューには次のファンクションがあります。

View System Eventlog (text, newest first)(システムイベントログの表示 (テキスト、新しいものから))	システムイベントログの内容が可読の形式で、入力時期の新しいものから順に画面に出力されます。
View System Eventlog (text, oldest first)	イベントログの内容が可読の形式で、入力時期の古いものから順に画面に出力されます。
Dump System Eventlog (raw, newest first) (イベントログのダンプ (画像、新しいものから))	イベントログの内容が入力時期の新しいものから順にダンプされます。
Dump System Eventlog (raw, oldest first) (イベントログのダンプ (画像、古いものから))	イベントログの内容が入力時期の古いものから順にダンプされます。

表 14: システムイベントログのメニュー

システムイベントログ情報の表示	システムイベントログの情報を表示します。
Clear System Eventlog (システムイベントログの消去)	システムイベントログの内容を消去します。
Change System Eventlog mode	システムイベントログのバッファモードを *リング* バッファモードから *リニア*バッファモードに、またはこの逆に変更します。

表 14: システムイベントログのメニュー

Internal Eventlog

「*Enclosure Information...*」サブメニューから「*Internal Eventlog*」を選択すると、次のメニューが表示されます。

```
    Internal Eventlog Menu

(1) View Internal Eventlog (text, newest last)
(2) Dump Internal Eventlog (raw, newest last)
(3) View Internal Eventlog Information
(4) Clear Internal Eventlog
(5) Change Internal Eventlog mode

Enter selection or (0) to quit:
```

図 193: リモートマネージャ : 「Internal Eventlog」メニュー

サブメニューには次のファンクションがあります。

View Internal Eventlog (text, newest last)	内部イベントログの内容が可読の形式で、入力時期の古いものから順に画面に出力されます。
Dump Internal Eventlog (raw, newest last)	内部イベントログの内容が入力時期の古いものから順にダンプされます。
View Internal Eventlog Information	内部イベントログの情報を表示します。
Clear Internal Eventlog	内部イベントログの内容を消去します。
Change Internal Eventlog mode	イベントログ内容 のバッファモードを *リングバッファモード*から *リニアバッファモード*に、またはこの逆に変更します。

表 15: 「Internal Eventlog」メニュー

8.11 サービスプロセッサ - IP パラメータ、識別灯、iRMC S4 リセット

メインメニューから「*Service Processor...*」を選択すると、次のメニューが表示されます。

```
    Service Processor Menu

(1)  Configure IP Parameters
(2)  List IP Parameters

(3)  Toggle Identify LED

(4)  Reset iRMC S2 (Warm reset)
(5)  Reset iRMC S2 (Cold reset)

Enter selection or (0) to quit:
```

図 194: リモートマネージャ : 「Service Processor」メニュー

サブメニューには次のファンクションがあります。

IP パラメータの設定	iRMC S4 の IPv4/IPv6 アドレス設定をガイド付きダイアログで設定します。個々の設定の詳細は、230 ページ の「Network Interface - iRMC S4 上の Ethernet 設定の編集」の項を参照してください。
P パラメータのリスト	IP パラメータを表示します。
識別灯のトグル	PRIMERGY の識別灯のオン / オフを切り替えます。
Reset iRMC S4 (Warm reset)	iRMC S4 をリセットします。接続が閉じられます。インターフェースだけが再初期化されます。
Reset iRMC S4 (Cold reset)	iRMC S4 をリセットします。接続が閉じられます。iRMC S4 全体が再初期化されます。

表 16: サービスプロセッサのメニュー

i 「*Reset iRMC S4（Cold Reset）*」または「*Reset iRMC S4（Warm Reset）*」の後にサーバを再起動することを推奨します（185 ページを参照）。

8.12 RAID Management

メインメニューから「*RAID Management...*」を選択すると、次のメニューが表示されます。

```
    RAID Management Menu

(1) Controller information
(2) Physical device information
(3) Logical device information
(4) Array configuration information
(5) BBU status

Enter selection or (0) to quit:
```

図 195: リモートマネージャ : 「Service Processor」メニュー

サブメニューには次のファンクションがあります。

Controller Information	管理対象サーバの各 RAID コントローラに関する情報を表示します。
Physical Device Information	管理対象サーバの各 RAID 物理ディスクに関する情報を表示します。
Logical Device Information	管理対象サーバの各 RAID 論理ドライブに関する情報を表示します。
Array configuration information	アレイ設定に関する情報を表示します。
BBU status	バッテリーバックアップユニット（BBU）のステータス情報を表示します。

表 17: サービスプロセッサのメニュー

8.13 Console Redirection (EMS/SAC) - テキストコンソールリダイレクションの開始

メインメニューの「*Console Redirection (EMS/SAC)*」項目からコンソールリダイレクションを開始できます。

> テキストベースのコンソールリダイレクションは、シリアル 1 の LAN 上でのみ動作します。
>
> コンソールリダイレクションを OS の実行中にも使用する場合は、「*Serial 1 Multiplexer*」を「*System*」に設定する必要があります。

> <ESC> + <(> または <~> + <.>（チルド + ドット）キーでテキストコンソールを終了します。
>
> 使用する PRIMERGY サーバのタイプによっては、このオプションのうちの 1 つだけが機能します。

8.14 コマンドラインシェルの起動 ...- SMASH CLP シェルの起動

コマンドラインシェルの起動 ...（メインメニュー）で、SMASH CLP シェルを起動できます。SMASH CLP は、「**S**ystems **M**anagement **A**rchitecture for **S**erver **H**ardware **C**ommand **L**ine **P**rotocol」の略語です。このプロトコルにより、管理端末と管理対象サーバとの Telnet または SSH ベース接続が可能になります。SMASH CLP に関して詳しくは、328 ページ の「コマンドラインプロトコル (CLP)」の項 を参照してください。

メインメニューから *(s) Start a Command Line shell...* を選択すると、次のウィンドウが現われます。

```
    Shell Menu

(1) Start SMASH CLP shell...


Enter selection or (0) to quit:
```

図 196: リモートマネージャ : 「Start a SMASH CLP shell... 」メニュー

► *(1) Start a SMASH CLP shell...* を選ぶと、SMASH CLP シェルが起動します。

8.15 Console Logging - メッセージ出力のテキストコンソールへのリダイレクト（シリアル）

メインメニューの「*Console Logging*」項目では、メッセージ出力（ログ）をテキストコンソールにリダイレクトできます（シリアルインターフェース）。

メインメニューから「*(l) Console Logging*」を選択すると、次のウィンドウが表示されます。

```
    Console Logging Menu

(1)  Change Logging Run state
(2)  Clear Console Logging buffer
(3)  Replay Console (Fast mode)
(4)  Replay Console (Continuous mode)

Enter selection or (0) to quit:
```

図 197: リモートマネージャ : 「Console Logging」メニュー

サブメニューには次のファンクションがあります。

Change Logging Run state	ログ実行状態を表示し、変更します。 詳細は、327 ページ の「「Console Logging Run State」メニュー」を参照してください。
Clear Console Logging buffer	コンソールログバッファを削除します。
Replay Console (Fast mode)	コンソールログを表示します（高速モード）。
Replay Console (Continuous mode)	コンソールログを表示します（連続モード）。

表 18: 「Console Logging」メニュー

「Console Logging Run State」メニュー

```
    Console Logging Run State Menu
    State: STOPPED (Normal Mode)

(r) Start Console Logging
(*) Stop Console Logging

(t) Toggle to Text Mode
(*) Toggle to Normal Mode

Enter selection or (0) to quit:
```

図 198: リモートマネージャ : 「Console Logging Run State」メニュー

「*Console Logging Run State Menu*」には次の機能があります。

「*Start Console Logging*」	メッセージのテキストコンソールへの出力を開始します。
「*Stop Console Logging*」	メッセージのテキストコンソールへの出力を停止します。
「*Toggle to Text Mode*」	テキストモードに切り替えます。 メッセージがコンソールに出力される前に、すべてのエスケープシーケンスは除外されます。
「*Toggle to Normal Mode*」	ノーマルモードに切り替えます。 ノーマルモードでは、メッセージがコンソールに出力される前に、次のエスケープシーケンスのみが除外されます。 <ESC>(<ESC>stop <ESC>Q <ESC>R<ESC>r<ESC>R <ESC>^ これは、色、擬似グラフィックスなどを一定の限度まで表現できることを示します。

表 19: 「Console Logging Run State」メニュー

8.16 コマンドラインプロトコル (CLP)

iRMC S4 はユーザシェルと呼ばれるさまざまなテキストベースのユーザインターフェースをサポートし、各ユーザ向けに設定できます。

Systems **M**anagement **A**rchitecture for **S**erver **H**ardware (SMASH) イニシアティブは、下記の目標のもとにいくつかの仕様を定義しています。

– 異質 (ヘテロジニアス) なコンピュータ環境を管理するための標準化されたインターフェースの提供。
– 統一的なインターフェース、ハードウェアおよびソフトウェア発見、リソースアドレッシング、データモデルをそなえたアーキテクチャフレームワークの提供。

SMASH に関する詳しい情報は下記のリンクで見ることができます。

http://www.dmtf.org/standards/smash

SMASH CLP シンタックス

SMASH CLP は、インターネット上で、また企業およびサービスプロバイダー環境で、コンピュータを管理するための共通コマンドラインシンタックスとメッセージプロトコルセマンティックスを指定します。SMASH CLP に関する詳細情報は、DMTF ドキュメント『Server Management Command Line Protocol Specification (SM CLP) DSP0214』で参照できます。

CLP の一般的シンタックス (構文) は次の通りです。

```
<verb> [<options>] [<target>] [<properties>]
```

<verb>

Verb (動詞) は、実行すべきコマンドやアクションを指定します。動詞のリストは、たとえば、次のような活動を記述します。

– データの設定 (*set*) および検索 (*show*)、
– ターゲットの状態の変更 (*reset*, *start, stop*)、
– 現セッションの管理 (*cd*, *version*, *exit*) 、
– コマンドに関する情報の返送 (*help*)。

iRMC S4 システムでは、*oemfujitsu* という動詞が、OEM 専用コマンドの使用も可能にします。

<options>

コマンドオプションは、動詞のアクションまたは挙動を修正します。オプションはコマンドラインコマンドライン上で動詞の直後に続くことができ、常にダッシュ ("-") により導入されなければなりません。

オプションを使って、たとえば、次のことができます。

- 出力フォーマットの定義
- コマンドの反復実行の許可
- コマンドのバージョンの表示
- ヘルプの要求

<target>

target> (ターゲット) は、コマンドにより操作されるオブジェクトのアドレスやパス、すなわちコマンドのターゲットを指定します。ターゲットは単一の管理対象要素、たとえば、ハードディスク、ネットワークアダプタ (Network Interface Card, NIC)、あるいは、マネジメントプログラム (Management Assistance Program, MAP) 自体であることができます。しかしターゲットは、トランスポートサービスのようなサービスであることも可能です。

マネジメントプログラムにより管理できる複数の管理対象要素を、単一の <target の下に包摂することができます。たとえば、システム全体というターゲットです。

各コマンドにはひとつのターゲットしか指定できません。

<properties>

<properties> (プロパティ) は、コマンドを実行するよう要求されているターゲットのプロパティを記述します。こうして、<properties> は、コマンドにより検索または修正されるターゲットのクラスのプロパティを特定します。

CLP 内のユーザデータ (概要)

CLP 内のデータは階層構造をなしています。コマンド *cd* を使うと、この構造内を移動することができます。

CLP 内のユーザデータの概要を 図 199 に示します。長方形で囲った名前は、コマンドターゲットを示します。階層のいずれのレベルでも、コマンド / 動詞 *show* が、利用可能なターゲット、プロパティ、および動詞を表示します。

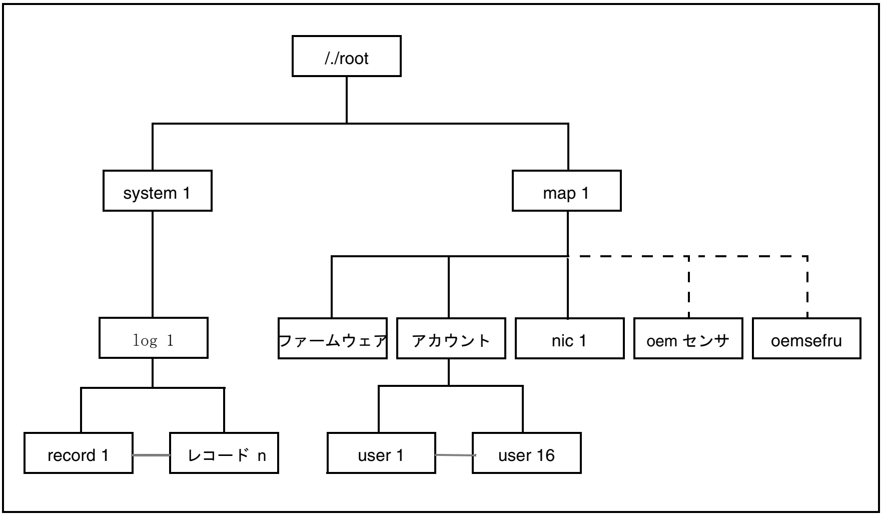


図 199: SMASH CLP 内のユーザデータの構造

CLP コマンドの階層

CLP コマンド階層の概要を 331 ページ の表 20 に示します。

Target \ Verb	Properties	Comment	cd	show	help	exit	version	set	reset	start	stop	load	oemfsc
// **system1** **map1**		Root	X	X	X	X	X						
system1	name enabledstate	Host System	X	X	X	X	X		System	PON	POFF		
...log1		Event Log (SEL)	X	X	X	X	X		iRMC				X
....record<n>	number date time sensordescription eventdescription eventdirection	Single SEL entry	X	X	X	X	X		iRMC				X
map1	name	iRMC	X	X	X	X	X		iRMC				X
...firmware	version	iRMC FW	X	X	X	X	X		iRMC			X	X
...accounts		Accounts	X	X	X	X	X	X	iRMC				X
......user<n>	username password group	User	X	X	X	X	X	X	iRMC				X
...nic1	networkaddress oemfsc_nonvol_networkaddress oemfsc_mask oemfsc_nonvol_mask oemfsc_gateway oemfsc_nonvol_gateway oemfsc_dhcp_enable oemfsc_nonvol_dhcp_enable oemfsc_vsi_path oemfsc_vsi_server oemfsc_vsi_permission oemfsc_vsi_sustain	LAN	X	X	X	X	X	X	iRMC				X
...oemfsc_sensors		OEM Sensors	X	X	X	X	X		iRMC				X
.....oemfsc_sensor_num<n>lun<m>	oemfsc _reading oemfsc _status oemfsc _sensortype oemfsc _readingtype	Single Sensor	X	X	X	X	X		iRMC				X
...oemfsc_frus		FRU	X	X	X	X	X		iRMC				X
.....oemfsc_fru_devid<n>lun<m>	oemfsc _description	Single FRU	X	X	X	X	X		iRMC				X

表 20: CLP コマンドの階層

9 Server Configuration Manager を使用した iRMC S4 の設定

Server Configuration Manager を使用して、次のことを実行できます。

- 管理対象サーバでの iRMC S4 を使用した消費電力管理の設定
- 管理対象サーバでの iRMC S4 を使用した電源冗長構成
- AVR タイトル、ライセンスキー、iRMC S4 のその他の機能の設定
- iRMC S4 時間設定
- バーチャルメディアを提供するための iRMC S4 の設定
- iRMC S4 DNS 登録の設定
- iRMC S4 DNS サーバの設定
- iRMC S4 E-mail 通知の設定
- iRMC S4 E-mail フォーマット設定
- iRMC S4 SNMP 通知の設定
- iRMC S4 に関するローカルユーザ管理の設定
- iRMC S4 のディレクトリサーバの設定
- iRMC S4 での CAS サービスの設定

> **i** **要件** :
>
> 管理対象サーバには最新の ServerView エージェントをインストールしておく必要があります。

次のようにして、Server Configuration Manager 機能にアクセスできます。

- ServerView Installation Manager を使用して管理対象サーバでローカルにアクセスする
- Windows のスタートメニューを使用して管理対象の Windows ベースサーバでローカルにアクセスする

  > **i** これは Windows 用 ServerView エージェントがインストールされているサーバでのみサポートされます。

- Operations Manager のグラフィカルインターフェースを使用してリモートワークステーション上でアクセスする

これは Windows 用 ServerView エージェントがインストールされているサーバでのみサポートされます。

この章では、Server Configuration Manager を呼び出すさまざまな方法について説明します。

Configuration Manager ダイアログページの詳細は、Server Configuration Manager のオンラインヘルプを参照してください。

9.1 ServerView Installation Manager からの Server Configuration Manager の呼び出し

Server Configuration Manager は、ServerView Installation Manager（短縮して Installation Manager）から呼び出せます。サーバをインストールする際、Installation Manager からの設定が重要になります。Installation Manager によって、インストールの準備中、およびメンテナンスプログラムとして、Server Configuration Manager を使用できるようになります。Installation Manager については、『ServerView Installation Manager』マニュアルに記載されています。

9.2 Windows スタートメニューからの Server Configuration Manager の呼び出し

Windows ベースのサーバでは、Windows スタートメニューからも Server Configuration Manager を呼び出せます。

これは次の手順で行います。

▶ 管理対象サーバで、次のように選択します。
「*Start*」–「*All Programs*」–「*Fujitsu*」–「*ServerView* 」–「*Agents* 」「*Configuration Tools*」–「 *System Configuration*」。

「*システム設定*」ウィンドウが開きます。

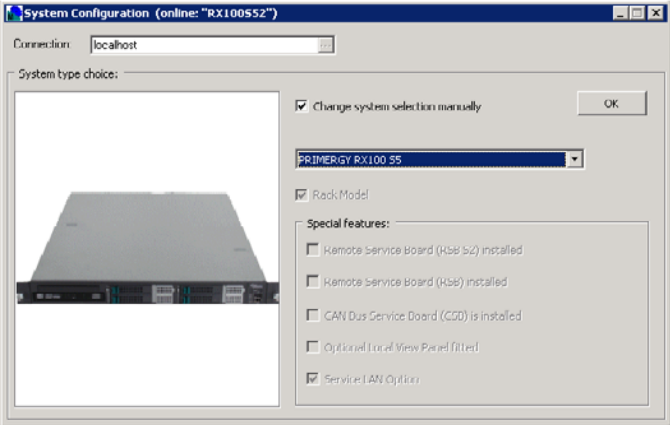


図 200: 「システム設定」ウィンドウ

- 設定済みの値を使用します。
- 「*OK*」をクリックします。

  「*システム設定*」ウィンドウのタブビューが開きます。

  矢印をクリックして、左右のタブにスクロールできます。

設定の適用

個々のタブで指定した設定を適用するには、各タブで次の手順に従います。

- 「*適用*」ボタンをクリックします。
- 「*ページ保存*」ボタンをクリックします。

  iRMC S4 が自動的に再起動して、変更された設定が有効になります。

9.3 Operations Manager からの Server Configuration Manager の呼び出し

iRMC S4 を設定する Server Configuration Manager のダイアログボックスは、Operations Manager のグラフィカルユーザインターフェースからも使用できます。これによって、管理対象サーバの iRMC S4 を Web インターフェース経由でリモートワークステーションから設定できます。

次の手順に従います。

► Operations Manager を起動します（ServerView Operations Manager のマニュアルを参照）。

  Operations Manager の開始ウィンドウが開きます。

図 201: Operations Manager: 開始ウィンドウ

► Operations Manager の開始ウィンドウの「*管理者設定*」メニューから「*サーバ設定*」を選択します。

その結果、次のウィンドウが開かれます。

図 202: Operations Manager: 「サーバ設定」ウィンドウ - 「サーバリスト (1)」タブ

► 「サーバリスト」タブで、設定するタブを選択します。

その結果、次のウィンドウが開かれます。

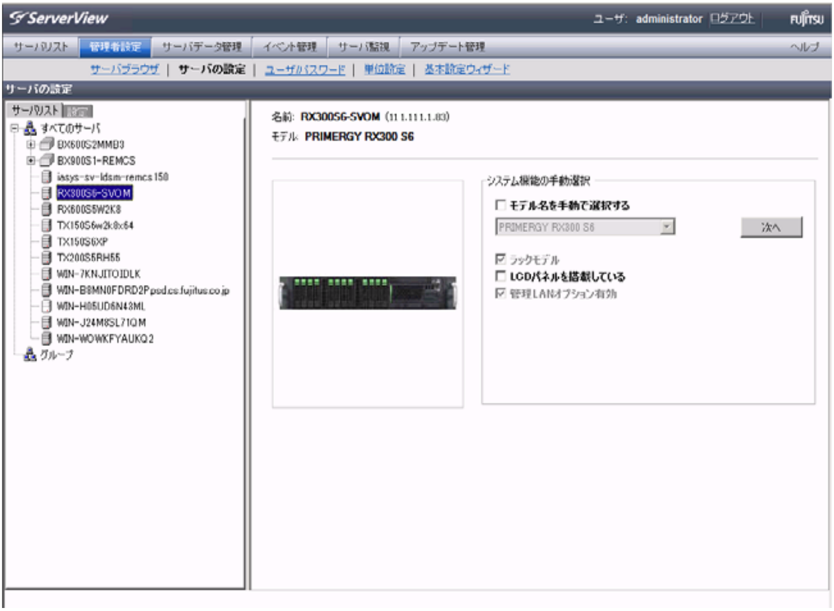


図 203: Operations Manager: 「サーバ設定」ウィンドウ - 「サーバリスト (2)」タブ

► ウィンドウの右側で、選択したサーバの詳細を指定して、「次へ」をクリックして入力内容を確定します。.

Server Configuration Manager の最初のダイアログが表示されます。

10 ファームウェアの更新

この章では次の点について説明します。

– iRMC S4 ファームウェア（概要）

– ファームウェアアップデート用メモリスティックの作成

– ファームウェアイメージのアップデート

– エマージェンシーフラッシュ

– フラッシュツール

注意！

ファームウェアをアップデートまたはダウングレードする際、ファームウェアを正常に操作するには、ランタイムファームウェアと SDR（Sensor Data Record）が両方とも同じファームウェアリリースに属することを確認してください。

現行バージョンのファームウェアは *ServerView Suite DVD* に格納されています。または Fujitsu Technology Solutions Web サーバのダウンロードセクションから手動でダウンロードすることもできます。

ServerView Suite DVD の最新バージョンは 2 か月ごとに入手できます。

ファームウェアのアップデートを実行するほかに、ファームウェアを以前のバージョンにダウングレードできます。

ファームウェアをアップデートまたはダウングレードする前に、新しいファームウェアに付属の注意書き（特に Readme ファイル）をよくお読みください。

10.1 iRMC S4 ファームウェア（概要）

iRMC S4 は 2 種類のファームウェアイメージを使用します。32 MB EEPROM（**E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory）にはそれぞれ 2 種類のファームウェアイメージが保存されています。

– ファームウェアイメージ 1 (低 FW イメージ)
– ファームウェアイメージ 2 (高 FW イメージ)

iRMC S4 のファームウェアは EEPROM では実行されず、起動時に SRAM メモリにロードされ、そこで実行されます。したがって、オンラインつまり Windows もしくは Linux といったサーバのオペレーティングシステムの実行中に、動作中のファームウェアと動作していないファームウェアの両方をアップデートすることができます。

i ファームウェアをイメージの 1 つからロードするときにエラーが発生した場合、ファームウェアはもう 1 つのイメージから自動的にロードされます。

i iRMC S4 ファームウェアと EEPROM に関する情報は、次の手段で取得できます。

– iRMC S4 Web インターフェースの「*iRMC S4 Information*」のページ（158 ページを参照）

– フラッシュツールの使用（356 ページを参照）

アクティブおよびパッシブファームウェアイメージ

常時 2 種類のファームウェアイメージのうちのどちらかが動作しています。どちらのファームウェアイメージが実行されるかは、いわゆるファームウェアセレクタが決定します (343 ページ参照)。

ファームウェアセレクタ

ファームウェアセレクタで、実行する iRMC S4 ファームウェアを指定します。iRMC S4 がリセットされて再起動されるたびに、ファームウェアセレクタが評価され、対応するファームウェアへのブランチを処理します。

ファームウェアセレクタには、次の値があります。:

0	ファームウェアバージョン最も新しいファームウェアイメージ
1	ファームウェアイメージ 1
2	ファームウェアイメージ 2
3	ファームウェアバージョンが最も古いファームウェアイメージ
4	更新時期が最も新しいファームウェアイメージ
5	更新時期が最も古いファームウェアイメージ

i どんな形の更新イメージを用いるかによって、更新後のファームウェアセレクタの設定は異なります。

ファームウェアセレクタは、

– iRMC S4 Web インターフェースの「*iRMC S4 Information*」ページでクエリを実行し、明示的に設定できます（160 ページ の「動作中ファームウェア」を参照）。

または

– フラッシュツールの使用（356 ページを参照）

10.2 USB メモリスティックの設定

iRMC S4 のファームウェアを次の方法でアップデートする場合は、USB メモリスティックは不要です。

- ServerView Update Manager を使用する
- ServerView Update Manager Express または ASP を使用する
- iRMC S4 Web インターフェースと TFTP サーバを使用する

次の手順に従います。

▶ ファームウェア *iRMC Firmware Update for USB Stick* を Fujitsu Technology Solutions Web サーバのダウンロードセクションから、コンピュータのディレクトリにダウンロードします。

ZIP アーカイブ *FTS_<spec>.zip* がダウンロードディレクトリに配置されます（名前の *<spec>* の部分には、システムタイプ、システムボード、ファームウェア /SDRR バージョンなどの情報が指定されます）。

ZIP アーカイブには次のファイルが格納されています。

- *USBImage.exe*
- *iRMC_<Firmware-Version>.exe*
- *iRMC_<Firmware-Version>.IMA*

▶ USB メモリスティックをコンピュータに接続します。

▶ ファイル *iRMC_<Firmware-Version>.exe* またはファイル *USBImage.exe* を起動します。

起動したファイルに応じて、次のうちの 1 つのウィンドウが開きます（345 ページ の図 204 を参照）。

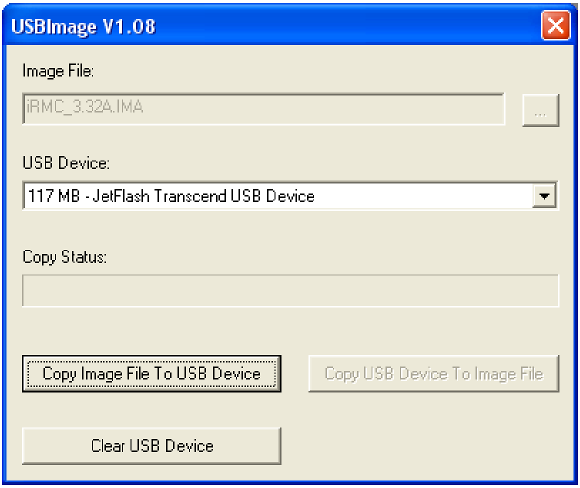


図 204: イメージファイルを USB メモリスティックにコピーする
（iRMC_<Firmware version>.exe を使用）

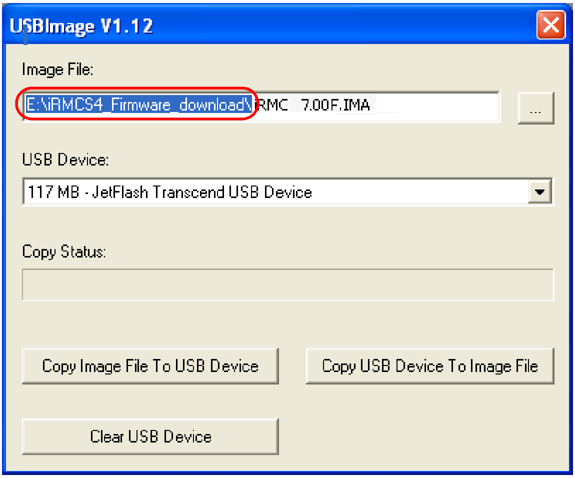


図 205: イメージファイルを USB メモリスティックにコピーする
（USBImage.exe を使用）

USBImag.exe を起動した場合、「*イメージファイル名*」で、ファイル *iRMC_<Firmware-Version>.IMA* を明示的に指定する必要があります。

► 「*Clear USB Device*」をクリックして、データを USB メモリスティックから削除します。

► 「*Copy Image File to USB Device*」をクリックして、ファイル *BMC_<Firmware-Version>.IMA* を USB メモリスティックにコピーして展開します。

注意！

この操作によって、USB メモリスティックの内容が上書きされます。

コピー操作が終了したら、フラッシュツールとイメージファイルが USB メモリスティックに格納されます。

Name	Size	Type	Date Modified
FDOS		Dateiordner	26.09.2012 10:26
MENU		Dateiordner	26.09.2012 10:26
700F_317.bin	30.720 KB	BIN-Datei	29.07.2013 11:43
Autoexec.bat	1 KB	Stapelverarbeitung...	09.11.2007 15:02
CHECK.EXE	15 KB	Anwendung	19.05.2009 10:44
clibmc.bat	1 KB	Stapelverarbeitung...	08.03.2006 10:46
command.com	65 KB	Anwendung für MS-...	16.02.2007 13:29
config.sys	1 KB	Systemdatei	16.02.2007 14:40
CVT100.EXE	20 KB	Anwendung	06.08.1988 20:17
CVT100.SET	1 KB	SET-Datei	05.12.2002 15:06
DosYafuf.exe	183 KB	Anwendung	22.07.2013 08:01
flashm.bat	6 KB	Stapelverarbeitung...	29.07.2013 11:42
FLIRMCS4.EXE	42 KB	Anwendung	17.07.2013 09:08
IPMIVIEW.EXE	148 KB	Anwendung	03.05.2013 10:59
IPMIVIEW.INI	14 KB	Konfigurationseinst...	03.08.2010 14:20
KERNEL.SYS	45 KB	Systemdatei	16.02.2007 15:11
readme.txt	9 KB	Textdokument	26.07.2013 08:03
SLEEP.EXE	9 KB	Anwendung	25.02.1998 20:17
WBAT.INI	3 KB	Konfigurationseinst...	08.06.2004 14:12

図 206: USB メモリスティック内のイメージファイルとフラッシュツール

10.3 ファームウェアイメージのアップデート

iRMC S4 ファームウェアは iRMC S4 の SRAM メモリ内で実行されるため、アクティブなファームウェアとアクティブではないファームウェアの両方をオンラインで、サーバのオペレーティングシステムを実行したまま、アップデートできます。

ファームウェアイメージは、次の方法でアップデートできます。

– iRMC S4 Web インターフェースを使用する

– ServerView Update Manager を使用する

– ServerView Update Manager Express または ASP を使用する

– オペレーティングシステムのフラッシュツールを使用してアップデートする

i 新しいバージョンのブートローダを使用する場合、両方のファームウェアイメージが同じアップデートプロセス内で自動的にフラッシュされます。

ファームウェアを以前のバージョンにダウングレードする

ファームウェアのアップデートを実行するほかに、ファームウェアを以前のバージョンにダウングレードできます。

ファームウェアをダウングレードする最も簡単な方法は、以前のバージョンのファームウェアイメージを非アクティブなファームウェアイメージとして iRMC S4 の EEPROM に保存することです。この場合、ファームウェアセレクタをこの以前のバージョンイメージに設定し（178 ページを参照）、その後 iRMC S4 を再起動してファームウェアを有効にするだけです。

i 以降の項で説明する方法を使用して、ファームウェアをダウングレードすることもできます。この場合、以前のバージョンのファームウェアに基づいてファームウェアのアップデートを実行します。以降の項では、ダウングレードを実行するための特別な要件を個別に示しています。

10.3.1 iRMC S4 Web インターフェースを使用したアップデート

「*iRMC S4 ファームウェアアップデート*」ページでは、ファームウェアイメージをローカルまたはリモートワークステーション、ネットワーク共有、または TFTP サーバに指定して、iRMC S4 のファームウェアをアップデートできます（177 ページ の「iRMC S4 ファームウェアアップデート」の項を参照）。

10.3.2 ServerView Update Manager を使用したアップデート

ServerView Update Manager を使用して、グラフィカルユーザインターフェースまたはコマンドラインインターフェース（Windows および Linux）を経由して、iRMC S4 ファームウェアのアップデートを開始できます。ServerView Update Manager は、*ServerView Suite DVD* または管理サーバ上のアップデートリポジトリから、アップデートデータにアクセスします。管理サーバのアップデートリポジトリは、ダウンロードマネージャを使用して、または Fujitsu Technology Solutions Web サーバのダウンロードセクションから手動でダウンロードして、アップデートします。

ServerView Update Manager によるファームウェアアップデートの詳細は、ServerView Update Manager のマニュアルを参照してください。

10.3.3 ServerView Update Manager Express または ASP を使用するオンラインアップデート

Windows および Linux オペレーティングシステムでは、iRMC S4 ファームウェアを ServerView Update Manager Express のグラフィカルユーザインターフェースまたは ASP（Autonomous Support Package）コマンドインターフェースを使用してアップデートできます。

Windows では、対応する ASP-**.exe* ファイルをダブルクリックして、Windows エクスプローラから ASP を開始することもできます。

i **ファームウェアをダウンロードする際は、次のことに注意してください。**

– Update Manager Express によるダウングレード :

ファームウェアダウングレードは*エキスパート*モードでのみ実行できます。また、*Downgrade* オプションも有効にする必要があります。

– ASP によるダウングレード :

– Windows の場合 :

ダウングレードは、対応する **.exe* ファイルをダブルクリックして ASP を開始して実行できます。ASP を CLI から開始する場合、*Force=yes* オプションを明示的に指定する必要があります。

– Linux の場合 :

オプション *-f* またはオプション *--force* を明示的に指定する必要があります。

Update Manager Express と ASP によるファームウェアアップデートの詳細は、ServerView Suite マニュアルの「Local System Update for PRIMERGY Servers」を参照してください。

10.3.4 オペレーティングシステムのフラッシュツールを使用してアップデートする

オペレーティングシステムのフラッシュツールを使用したオンラインアップデートは、_ リカバリフラッシュとしてのみ実行され、バージョンチェックは実行されません。

前提条件：

フラッシュツールとファームウェアアップデートのファイルが、管理対象サーバのファイルシステム上にあることが必要です。

実行しているオペレーティングシステムに応じて、次のフラッシュツールの 1 つを使用します。

DOS:	flirmcs4
Windows：	winflirmcs4 **前提条件：** 使用している Windows オペレーティングシステム（32/64 ビット）の ServerView エージェントが管理対象サーバで実行している必要があります。
Windows（32 ビット）：	w32flirmcs4（エージェントは不要）
Windows（64 ビット）：	w64flirmcs4（エージェントは不要）
Linux：	linflirmcs4

フラッシュツールを Windows コマンドライン（flirmcs4、w32flirmcs4、w64flirmcs4、winflirmcs4）または Linux CLI（linflirmcs4）で呼び出します。

フラッシュツールの構文とオペランドは、356 ページ の「フラッシュツール」の項に記載されています。

次の手順に従います。

> i USB メモリスティックを使用したオンラインアップデートは、以下で説明されています（344 ページ の「USB メモリスティックの設定」の項を参照）。

- ► USB メモリスティックを管理対象サーバに接続します。
- ► Windows コマンドラインまたは Linux コマンドラインインターフェース（CLI）で、USB メモリスティックに対応するドライブに移動します。
- ► フラッシュツールをパラメータ */s 4* で呼び出して、ファームウェアセレクタを値 4 に設定します。

  Windows コマンドラインでは、次のように入力します。

  `w32flirmcs4 /b 4` または `w64flirmcs4 /b 4`

- ► フラッシュツールを対応するアップデートファイルで呼び出して、ファームウェアと SDR データのアップデートを開始します。

  Windows コマンドラインでは、次のように入力します。

  `w32flirmcs4 *.bin /i` または `w64flirmcs4 *.bin /i`

  これにより、新しいバージョンを非アクティブな EEPROM にフラッシュします。

  > i ファームウェアと SDR は同じ **.bin* ファイルからフラッシュされます。

  > i */wr* パラメータを使用してフラッシュツールを呼び出す場合、フラッシュが完了すると、アップデートされたファームウェアが自動的にアクティブになります。この場合、iRMC S4 を再起動する必要はありません。

  ファームウェアのアップデート中、コンソールにはアップデート処理の進行状況が通知されます。エラーが発生した場合、アップデート処理は中止され、対応するリターンコードが報告されます（359 ページを参照）。

- ► 管理対象サーバを再起動しますこれによって、アップデートされたファームウェアのファームウェアイメージが自動的に有効になります。

10.3.5 FlashDisk メニューによるアップデート

FlashDisk メニューによるアップデートの場合は、起動可能な USB メモリスティックが必要です（344 ページ の「USB メモリスティックの設定」の項を参照）。

次の手順に従います。

▶ USB メモリスティックを管理対象サーバに接続します（直接、またはリモートストレージとして）。

▶ USB メモリスティックから起動します。

起動処理が完了した後、USB メモリスティックのデータは自動的に RAM ディスクにコピーされます。*autoexec.bat* ファイルが自動的に起動します。

FlashDisk メニューが開きます。

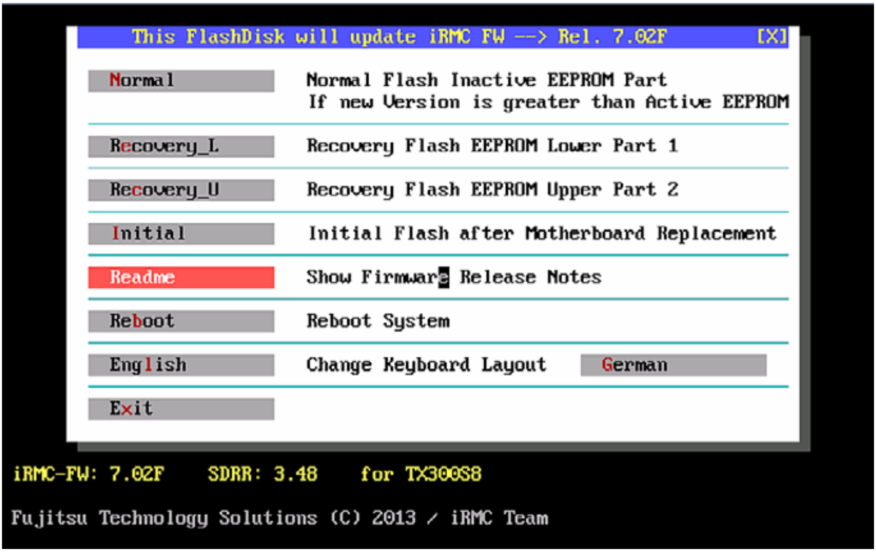


図 207: FlashDisk メニュー

ファームウェアダウングレードは、リカバリフラッシュによってのみ可能です。

「*Normal*」

*通常のフラッシュ*が実行されます。

通常のフラッシュ処理中、アクティブなファームウェアを含む EEPROM の領域が最新であるかどうかチェックされます。これらの領域で最新でないものがある場合、最新ではない、非アクティブなファームウェアに対応する領域がアップデートされます。

「*Recovery _L*」

ファームウェアイメージ 1（低ファームウェアイメージ）の *リカバリフラッシュ*が実行されます。

リカバリフラッシュの場合、ファームウェアイメージ 1 の 3 つの領域すべてについてフラッシュが実行され、バージョンチェックは実行されません。

「*Recovery _U*」

ファームウェアイメージ 2（高ファームウェアイメージ）の *リカバリフラッシュ*が実行されます。

リカバリフラッシュの場合、ファームウェアイメージ 2 の 3 つの領域すべてについてフラッシュが実行され、バージョンチェックは実行されません。

「*Initial* 」

アクティブなファームウェアと非アクティブなファームウェアの両方がフラッシュされます。

「*Readme*」

Readme ファイルが開きます。

「*リブート* 」

iRMC S4 ウォームスタートが実行されます。

「*English*」／「*German*」

キーボードレイアウトを指定します。デフォルトで「*German*」が設定されています。

► 対応するボタンをクリックして、必要な種類のアップデートを開始します。

ファームウェアのアップデート中、コンソールにはアップデート処理の進行状況が通知されます。エラーが発生した場合、アップデート処理は中止されます。対応するリターンコードが報告されます（359 ページを参照）。

► アップデート処理が完了したら、「*Exit*」をクリックして FlashDisk メニューを終了します。

► USB メモリスティックを管理対象サーバから取り外します。

► 管理対象サーバを再起動します（[Crtl]+[Alt]+[Del] を押します）。

10.4 エマージェンシーフラッシュ

SDR にシステムとの互換性がなくなり、iRMC S4 のファームウェアが実行できなくなった場合、エマージェンシーモードを使用してファームウェアを再度実行させることができます。緊急時モードでは、システムは自動的にブートローダに分岐して、ファームウェアアップデート用に準備されます。

i 緊急時モードは、エラー LED（前面保守 LED）（赤色）と識別灯（青色）が交互に点滅して示されます。

管理対象サーバを緊急時モードに切り替えて iRMC S4 のファームウェアをアップデートするには、次の手順に従います。

► 電源コネクタを取り外します。

► ID キーを押し下げて、コネクタをソケットに接続し直します。

管理対象サーバが緊急時モードになります。

► サーバで DOS を起動し、リカバリフラッシュ手順を使用して iRMC S4 のファームウェアをアップデートします。

i ファームウェアがアクティブではない場合、起動処理の開始までに最高 2 分かかります。このの期間中に BIOS から出力されるエラーメッセージ「iRMC S4 Controller Error」は無視できます。

10.5 フラッシュツール

flirmcs4、w64flirmcs4、linflirmcs4、w32flirmcs4 は、呼び出される環境によって名前のみが異なります。つまり、下記の説明は、これらのツールにみ当てはまります。「w32flirmcs4」の代わりに、「flirmcs4」、「w64flirmcs4」、「linflirmcs4」のいずれかを必要に応じて入力します。

構文

```
w32flirmcs4 <filename> [<Option>]...
```

<Filename> フラッシュオプションなし：ファームウェアをアップデート /u と同じ）

オプション

/h または /? このヘルプ情報を表示します

/v 「w32flirmcs4」の実際のプログラムバージョンを表示します

/vNoDriverLoad 「w32flirmcs4」の実際のプログラムバージョンを表示します

/o ファームウェアの実際のリビジョンを表示

/1 バージョンをチェックして 1 つ目の EEPROM をフラッシュ

/2 バージョンをチェックして 2 つ目の EEPROM をフラッシュ

/f1 バージョンをチェックせずに 1 つ目の EEPROM を強制的にフラッシュ

/f2 バージョンをチェックせずに 2 つ目の EEPROM を強制的にフラッシュ

/fi バージョンをチェックせずに非アクティブな EEPROM を強制的にフラッシュ

/i バージョンをチェックして非アクティブな EEPROM をフラッシュ

/u 新しいバージョンがアクティブな EEPROM より大きい場合、非アクティブな EEPROM をフラッシュ

/wr ファームウェアのウォームリセットを開始

/s [0-2] FW Upload Selector を表示 / 設定

0 : 自動、非アクティブイメージ

1 : イメージ 1、低ファームウェアイメージ

2 : イメージ 2、高ファームウェアイメージ

/b [0-5] Show/Set FW Boot Selector

0 : 自動、より新しいファームウェアバージョンを選択

1 : イメージ 1、低ファームウェアイメージ

2 : イメージ 2、高ファームウェアイメージ

3 : より低いファームウェアバージョンを自動選択

4 : プログラムされた最新のファームウェアを自動選択

5 : プログラムされた最古のファームウェアを自動選択

/n コンソール出力なし、ユーザの入力不要

/noUserEntry ユーザの入力不要、コンソール出力あり

/logError[file] エラーをログファイルに書き込む。デフォルト：w32flirmcs4.logError

/logOutput[file] 各端末の出力をログファイルに書き込む。

デフォルト：w32flirmcs4.logOutput

/logDebug[file] 各内部デバッグの出力をログファイルに書き込む。

デフォルト：w32flirmcs4.logDebug

/ignore   チェックなしで選択した EEPROM をフラッシュ (FW バージョン、SDR ID）

/d [0-99] [0-99] 追加のデバッグ出力 [冗長レベル]

a）冗長レベルなし：デバッグ全体の出力をプリント

b）冗長レベル 1：デバッグ出力をプリント <= 冗長レベル

c）冗長レベル 2：冗長レベル 1 と 2 の間で、デバッグ出力をプリント

/e   テストモードをエミュレート（RMC にアクセスしない、テストのみ）

/noExitOnError エラーの後、終了せずにプログラムを継続（テストのみ）

99：EEPROM ファームウェアが動作中のため、フラッシュしない

リターンコード

値	意味
00	エラーなし。プログラムは正常終了した。
01	引数がないまたは不適切。
02	ファームウェアアップロードセレクタが範囲外（0-2）。
03	ファームウェアブートセレクタが範囲外（0-5）。
04	ファームウェアイメージファイルがない。
05	ファームウェアイメージファイルを開けない。
06	BMC での通信ができない。
07	IPMI コマンドの完了コードが不適切。
08	システムに iRMC S4 がない。
09	システムとフラッシュイメージファイルの の SDR ID が同じでない。
10	メモリバッファを割り当てることができない。
11	ファイル転送に失敗した。
12	IPMI 呼び出しに失敗した（レスポンスデータサイズが 0）。
13	HTI インターフェースを使用できない。
14	HTI インターフェースの検出に失敗した（他の検出エラー）
15	HTI インターフェースの検出に失敗した（ScSBB2.sys ドライバを使用できない）
16	HTI への接続に失敗した。
17	フラッシュプロセスに失敗した。
18	[F5 0B Start TFTP Flash] のエラー完了コード：0xCB。 データが存在しない（TFTP サーバがリクエストされたイメージファイルを提供できなかった）。
19	[F5 0B Start TFTP Flash] のエラー完了コード：0xD3。 宛て先を使用できない（TFTP サーバが到達できない）。
20	[F5 0B Start TFTP Flash] の完了コードが未知。
21	ファームウェアイメージファイルのファイルサイズが不適切。
22	ファームウェアイメージファイルでの検索エラー。
23	GetFullPathName に失敗しました。
24	フラッシュステータスが 0x04（イメージのダウンロードが進行中）のため、イメージをロードできない。
25	フラッシュステータスが 0x08（フラッシュが進行中）のため、イメージをロードできない。

表 21: フラッシュツールのリターンコード

値	意味
26	ファイルのロード前に予期しない iRMC のフラッシュステータス。
27	ファームウェアイメージファイルが存在しない。
28	予期しない IPMI コマンドのレスポンスデータサイズ。
29	HTI 関数から予期しない戻り値。
30	オペレーティングシステムでこのアプリケーションプログラムを実行できない。

表 21: フラッシュツールのリターンコード

11　iRMC S4 によるオペレーティングシステムのリモートインストール

本章では、ServerView Installation Manager（以下 Installation Manager）および iRMC S4 の「ビデオリダイレクション（AVR)」および「バーチャルメディア」機能を使用して、リモートワークステーションから管理対象サーバ上にオペレーティングシステムをインストールする方法について、概要を説明します。

この章では、以下の特定のトピックについて説明します。

– 「バーチャルメディア」機能によってて提供されるストレージメディアを使用した、オペレーティングシステムのリモートインストールの一般的な手順。これ以降、「バーチャルメディア」機能によって提供されたストレージメディアは、略して仮想ストレージメディアと呼びます。

– ServerView Suite DVD（Windows および Linux）を使用してリモートワークステーションから管理対象サーバを起動します。

– 管理対象サーバに対する設定後にリモートワークステーションから Windows をインストールします。

– 管理対象サーバに対する設定後にリモートワークステーションから Linux をインストールする

仮想ストレージメディアの操作に主に焦点を当てて説明します。読者が Installation Manager の機能に精通していることを前提としています（『_ServerView Installation Manager』マニュアルを参照）。

i　**iRMC S4 を使用したオペレーティングシステムのリモートインストールの前提条件：**

– iRMC S4 の LAN インターフェースが設定されている必要があります
(39 ページを参照)。

– iRMC S4 の「ビデオリダイレクション（AVR)」機能と「バーチャルメディア」機能を使用するためのライセンスキーをインストールする必要があります（161 ページを参照）。

11.1 iRMC S4 を使用したオペレーティングシステムのインストール - 基本手順

Installation Manager の場合、iRMC S4 を使用したオペレーティングシステムのリモートインストールとは、バーチャルメディアを使用して、リモートワークステーションから AVR ウィンドウを介して、管理対象サーバ上にオペレーティングシステムをローカルに設定およびインストールすることです。

Installation Manager を使用したインストールを行うには、以下の手順が必要です。

1. 起動元にする仮想ストレージメディア（DVD または Installation Manager ブートイメージ）を仮想ストレージメディアとして接続します。
2. DVD または Installation Manager ブートイメージを使用して、管理対象サーバを起動し、設定します。
3. リモートワークステーションの Installation Manager を使用して、管理対象サーバにオペレーティングシステムをインストールします。

Installation Manager を使用せずに、Windows インストール CD/DVD で Windows をインストールする

バーチャルメディアによる Windows のリモートインストールは、Installation Manager を使用しても、Windows インストール CD/DVD のみを使用しても行えます。仮想ストレージメディアの操作に関しては、この 2 つの方法はどちらも同じです。

しかし、次の理由から、Installation Manager を使用して Windows をインストールすることをお勧めします。

– Installation Manager 自身が、必要なドライバを識別して _ システムにコピーします。
– インストール中に、Installation Manager のすべての機能を使用できます。つまり、たとえばサーバ管理設定も含め、システム全体を設定することができます。
– Installation Manager を使用しないインストールは、インストールプロセス中にマウスカーソルを同期できないため、キーボードで操作する必要があります。それとは対照的に、Installation Manager を使用してインストールすると、すべての設定手順およびインストール手順をマウスを使用して行うことができます。
– Installation Manager を使用しないでインストールすると、マウスカーソルの同期に必要なすべての設定を手動で行う必要があります。

– Installation Manager を使用したインストールの所要時間は、オペレーティングシステムの CD/DVD を使用したインストールと大差はありません。

Installation Manager を使用せずに、Linux インストール CD/DVD を使用して Linux をインストールする

システムが必要とするドライバがわかっている場合は、Linux インストール CD/DVD から起動して、Linux のインストールを開始できます。

インストールで、フロッピーディスクのドライバを統合する必要がある場合は、インストールを開始する前に、次のメディアとのバーチャルメディア接続をセットアップする必要があります。

– 起動元にするストレージメディア（CD-ROM/DVD-ROM または ISO イメージ）

– 必要に応じて、ドライバのインストール用ストレージメディア

11.2 バーチャルメディアとしてのストレージメディアの接続

バーチャルメディア機能を使用すると、ネットワークの他の場所にある「仮想」ドライブを利用できるようになります。

仮想ドライブのソースには、以下を使用できます。

– リモートワークステーションの物理ドライブまたはイメージファイルイメージファイルはネットワークドライブ（たとえば、D ドライブの場合「D:」ドライブ文字を使用）でも構いません。

– Remote Image Mount によってネットワークの中心に置かれるイメージファイル。

「バーチャルメディア」機能の詳細については、109 ページ の「仮想メディアウィザード」の章を参照してください。

リモートワークステーションで仮想ストレージメディア t ごしてストレージメディアを接続

リモートワークステーションで次の手順に従って、バーチャルメディア接続を確立します。

► 「Remote Storage Enabled」を許可して iRMC S4 Web インターフェースにログインします（120 ページを参照）。

► 「*AVR（Advanced Video Redirection：ビデオリダイレクション*」ページを開き、AVR を起動します（288 ページを参照）。

► AVR ウィンドウで「バーチャルメディア」を起動します（111 ページを参照）。

► 仮想ストレージメディアとして使用するストレージメディアを準備します（114 ページを参照）。

– Installation Manager を使用してインストールする場合：

  ServerView Suite DVD または Installation Manager ブートイメージ、およびオプションで、フォーマット済みの USB メモリスティック（ステータスバックアップメディアとして使用）を準備します。

– ベンダーのインストール CD/DVD でインストールする場合：Windows または Linux インストール CD/DVD、およびオプションドライバを準備します。

i ServerView Suite DVD 1 およびオペレーティングシステムインストール CD/DVD をイメージファイル（ISO イメージ）としてフォルダに保存して、そこから仮想ストレージメディアとして接続するか、Remote Image Mount を使用して接続することをお勧めします。

準備したストレージメディアは、「*Virtual Media*」ダイアログボックスに表示されます。

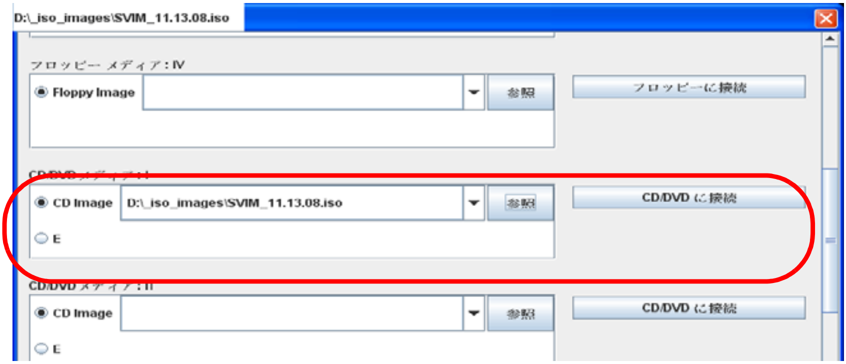


図 208: 「ストレージデバイス」ダイアログボックス：ServerView Suite DVD ISO イメージ

► 「*接続*」をクリックして、DVD ROM ドライブ（DVD）または Installation Manager ブートイメージをリ仮想ストレージメディアとして接続します。

Remote Image Mount によって提供された ISO イメージ（イメージファイル）の接続

Installation Manager ブートイメージからの起動に、Remote Image Mount を使用して提供されたイメージファイルを使用できます。

Remote Image Mount を使用してイメージファイルを提供する方法については、299 ページ の「「リモートイメージマウント」- リモート ISO イメージへの接続」の項を参照してください。

11.3 管理対象サーバを ServerView Suite DVD から起動して、Installation Manager で設定する

リモートワークステーションで、次の手順に従います。

▶ iRMC S4 Web インターフェースを使用して管理対象サーバを起動するか、サーバをリブートします（185 ページを参照）。AVR ウィンドウのブートプロセスの進行状況に従います。

管理対象サーバの BIOS POST フェーズでは、仮想ストレージメディアは USB 2.0 デバイスとして表示されます。仮想ストレージのストレージメディアは 、BIOS ブートシーケンスに次のエントリで表示されます。

– （物理）フロッピーディスクは、別エントリの「FTS RemoteStorage FD-(USB 2.0」と表示されます。

– 他のすべての仮想ストレージデバイスタイプは、共有エントリ「CD-ROM DRIVE」と表示されます。

i バーチャルメディアとして接続されている ローカル CD-ROM/DVD-ROM ドライブと CD-ROM/DVD-ROM ドライブの両方が管理対象サーバに存在する場合は、管理対象サーバは、仮想イメージによって提供される CD-ROM/DVD-ROM ドライブから起動します。

▶ サーバの起動中に [F2] を押します。

▶ UEFI セットアップで、ブートシーケンスを定義できる「ブート」メニューを開きます。

▶ 仮想ストレージメディアとして接続されている ServerView Suite DVD に対して、Boot Priority=1（最高の優先度）を指定します。

▶ 設定を保存して、UEFI セットアップを終了します。

管理対象サーバが、仮想ストレージとして接続されている ServerView Suite DVD から起動します。

i **システムが仮想ストレージメディア（ServerView Suite DVD または Installation Manager ブートイメージ）から起動しない場合は、次の手順に従います。**

▶ BIOS POST フェーズでストレージメディアが表示されるかどうか確認し、必要に応じてストレージメディアをバーチャルメディアとして接続します。

► 正しいブートシーケンスが指定されていることを確認します。

ServerView Suite DVD（仮想ストレージメディア）からの起動には、5 分程度かかります。ブートプロセス中は、ブートの進捗状況が表示されます。ブートプロセスが完了すると、Installation Manager スタートアップにダイアログボックスが表示され、ステータスバックアップ領域のメディア（ステータスバックアップメディア）を選択するように求められます。

► 「*Installation Manager mode*」で「*Standard mode*」を選択します。

► 設定データの保存先を、ローカルな交換可能データメディアとネットワークメディアのどちらにするか指定します。

> **i** ステータスバックアップオプションを選択しないで再起動すると、設定データがすべて失われるので注意してください。

「Status backup medium」

> **i** バックアップメディアは書き込み保護されません。
>
> システムの起動時には、USB スティックが USB ポートに接続されている必要があります。USB ポートに接続されていない場合にコンフィグレーションファイルを保存するには、USB スティックを接続して、ServerView Suite DVD から再起動します。

► 「*on local drive (floppy / USB stick)*」オプションを選択します。

► このオプションの右側にあるボックスで、該当ドライブを選択します。

Installation Manager ステータスディスク作成に関する詳細は、『ServerView Installation Manager』マニュアルを参照してください。

「Connecting the status medium and/or the installation media via the network」

► この目的に必要な共有を設定します。

> **i** 準備したコンフィグレーションファイルを格納したメディア、およびインストールメディアをネットワーク経由で使用できるようにしている場合は、このオプションを選択する必要があります。インフラストラクチャに応じて、一時 IP アドレスを DHCP 経由で取得することも、現在の Installation Manager セッションに対して IPv4 または IPv6 アドレスを手動で設定することもできます。

► 「*次へ*」をクリックして、Installation Manager を起動します。

ローカルインストールの開始

Installation Manager を起動すると、ようこそ画面が表示されます。

図 209: Installation Manager - ようこそ画面

► 「*Deployment*」をクリックして、ローカルインストール（デプロイメント）の準備を開始します。

インストールの準備を行うために、システム構成、およびその後の OS の自動インストールの仕様を収集する一連のコンフィグレーションステップが Installation Manager ウィザードによって提示されます。

> **i** 管理対象サーバのローカル CD ROM/DVD ROM ドライブをインストールソースとして設定します。また、リモートワークステーションの CD ROM/DVD ROM ドライブを仮想ストレージメディアとして管理対象サーバに接続すると、そのドライブから Windows インストール CD/DVD を使用できるようになります（370 ページ の「設定完了後の管理対象サーバへの Windows のインストール」の項を参照）。

Installation Manager での設定を完了すると、Windows インストール（370 ページを参照）または Linux インストール（372 ページを参照）の「*設定内容の確認*」ダイアログページが表示されます。このダイアログページからインストールプロセスを開始できます。

11.4 設定完了後の管理対象サーバへの OS のインストール

設定を完了したら、管理対象サーバにオペレーティングシステムをインストールする必要があります。

11.4.1 設定完了後の管理対象サーバへの Windows のインストール

設定が完了すると、次の _ ダイアログページが Installation Manager によって表示されます。

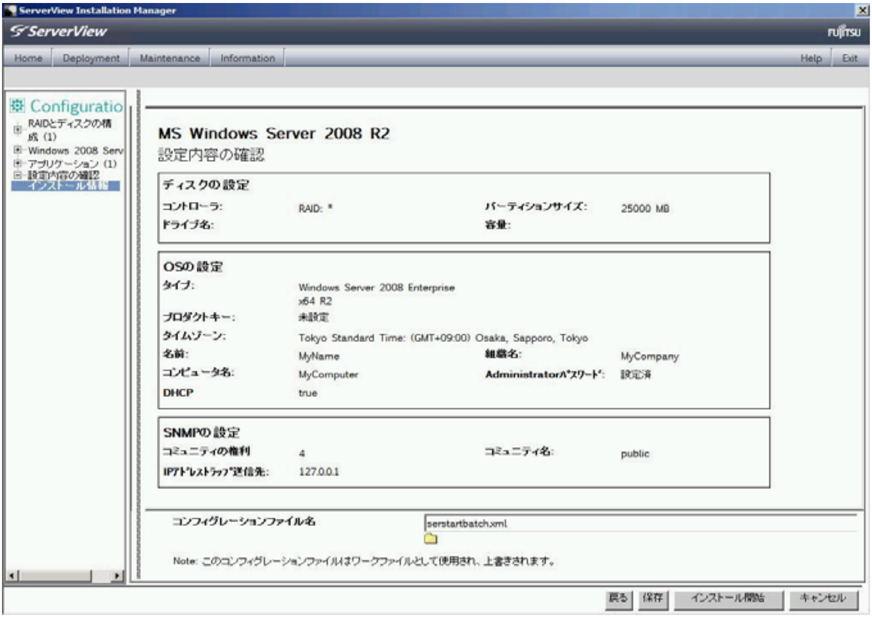


図 210: Installation Manager - 「設定内容の確認」ページ

管理対象サーバのローカル CD ROM/DVD ROM ドライブをインストールソースとして設定した場合は、リモートワークステーションで次の手順に従います。

► 現在アクティブなバーチャルメディア接続を解除します。バーチャルメディア接続の解除に関する詳細は、117 ページを参照してください。

► リモートワークステーションの DVD ROM ドライブから ServerView Suite DVD を取り出します。

► この DVD ROM ドライブに、Windows インストール CD/DVD を挿入します。

> **i** 「*autostart*」がアクティブな場合は、アプリケーションを閉じてください。

► Windows インストール CD/DVD が入っている CD ROM/DVD ROM ドライブを仮想ストレージとして接続します

► Installation Manager の「*設定内容の確認*」ページで、「*インストール開始*」をクリックします。

すべてのインストールファイルが、管理対象サーバにコピーされます。

コピー操作が完了すると、確認ダイアログページが Installation Manager によって開かれ、管理対象サーバを再起動する前にリムーバブルメディアドライブからすべてのストレージメディアを取り出すように求められます。

> **i** 具体的には、システムを再起動する前に、現在のバーチャルメディア接続をすべてシャットダウンする必要があります。

► 現在のバーチャルメディア接続をすべてシャットダウンするには、次の手順に従います。

  ► 「Virtual Media」を起動します（111 ページを参照）。

  「*Virtual Media* 」ダイアログが開き、現在接続されている仮想ストレージデバイスが表示されます。

  ► ストレージデバイスの 「安全な取り外し」を行います。つまり、ストレージデバイスにアクセスしているアプリケーションやプログラムがないことを確認してから取り外します。

  ► 「*切断*」ボタンをクリックして、すべての仮想ストレージ接続を解除します。

► 確認ダイアログページで、「*OK*」をクリックして管理対象サーバを再起動します。

管理対象サーバが再起動すると、AVR でインストール全体を監視できます。

11.4.2 設定完了後の管理対象サーバへの Linux のインストール

> **i** Linux のインストール中、マウスは使用できますが、同期はできません。

> **i** 仮想ストレージメディアを変更する場合は必ず、現在接続されているメディアの仮想ストレージメディア接続を取り外して、新しいメディアを仮想ストレージメディアとして接続する必要があります。

設定が完了すると、次の _ ダイアログページが Installation Manager によって表示されます。

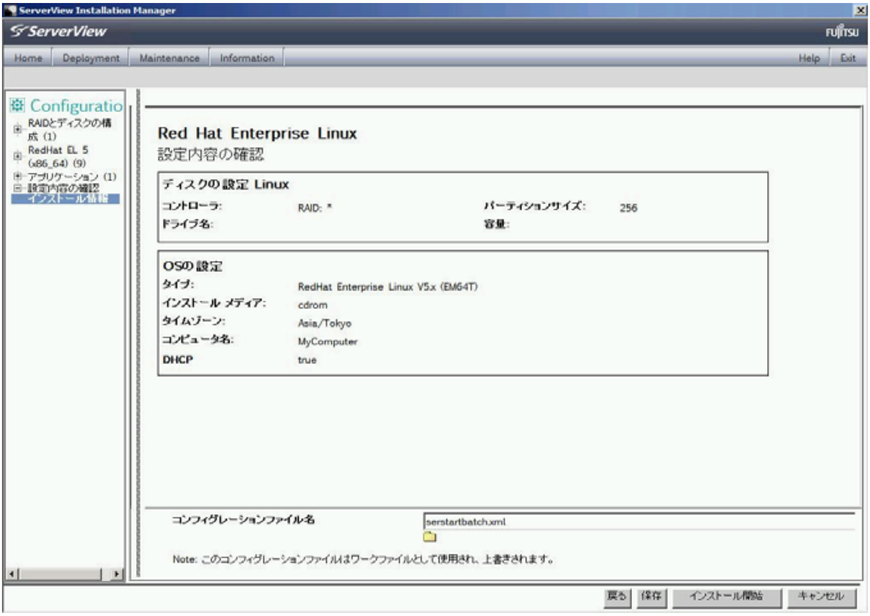


図 211: Installation Manager - 「設定内容の確認」

管理対象サーバのローカル CD ROM/DVD ROM ドライブをインストールソースとして設定した場合は、リモートワークステーションで次の手順に従います。

► 現在アクティブなバーチャルメディア接続を解除します。バーチャルメディア接続の解除に関する詳細は、117 ページを参照してください。

► リモートワークステーションで、ServerView Suite DVD を DVD ROM ドライブから取り外します。

► この DVD ROM ドライブに、Linux インストール CD/DVD を挿入します。

> i 「*autostart*」がアクティブな場合は、アプリケーションを閉じてください。

► Linux インストール CD/DVD が入っている CD ROM/DVD ROM ドライブを仮想ストレージとして接続します

► Installation Manager の「*設定内容の確認*」ページで、「*インストール開始*」をクリックします。

すべてのインストールファイルが、管理対象サーバにコピーされます。コピー操作が完了すると、確認ダイアログページが Installation Manager によって開かれ、管理対象サーバを再起動する前にリムーバブルメディアドライブからすべてのストレージメディアを取り出すように求められます。

> i 具体的には、システムを再起動する前に、現在のバーチャルメディア接続をすべてシャットダウンする必要があります。

► システムを再起動する前に、現在のバーチャルメディア接続をシャットダウンします。

これは次の手順で行います。

► 「Virtual Media」を起動します（111 ページを参照）。

「*Virtual Media*」ダイアログボックスが開き、現在接続されているバーチャルメディアデバイスが表示されます。

► 「*切断*」ボタンをクリックして、すべてのバーチャルメディア接続を解除します。

► ストレージデバイスの 「安全な取り外し」を行います。つまり、ストレージデバイスにアクセスしているアプリケーションやプログラムがないことを確認してから取り外します。

► 確認ダイアログページで、「*OK*」をクリックして管理対象サーバを再起動します。

管理対象サーバが再起動すると、AVR でインストール全体を監視できます。

12 付録

付録では次のトピックについて説明します。

– 375 ページ の「iRMC S4 でサポートされる IPMI OEM コマンド」
– 404 ページ の「SCCI およびスクリプト設定を使用した iRMC S4 の設定」

12.1 iRMC S4 でサポートされる IPMI OEM コマンド

本章では、iRMC S4 がサポートする OEM 特有の IPMI コマンドの選択について説明します。

12.1.1 概要

iRMC S4 では以下の OEM 特有の IPMI コマンドをサポートします。

- SCCI 準拠の自動電源投入／電源切断コマンド
  (SCCI: **S**erverView **C**ommon **C**ommand **I**nterface（ServerView 共通コマンドインターフェース））
  - 0115 Get Power On Source
  - 0116 Get Power Off Source
  - 011C Set Power Off Inhibit
  - 011D Get Power Off Inhibit
  - 0120 Set Next Power On Time
- **SCCI 準拠の通信コマンド**
  - 0205 System OS Shutdown Request
  - 0206 System OS Shutdown Request and Reset
  - 0208 Agent Connect Status
  - 0209 Shutdown Request Canceled
- **SCCI 準拠のシグナリングコマンド**
  - 1002 Write to System Display

- **Firmware 特有のコマンド**
  - 2004 Set Firmware Selector
  - 2005 Get Firmware Selector
  - C019 Get Remote Storage Connection
  - C01A Set Video Display on/off
- **BIOS 特有のコマンド**
  - F109 Get BIOS POST State
  - F115 Get CPU Info
- **iRMC S4 特有のコマンド**
  - F510 Get System Status
  - F512 Get EEPROM Version Info
  - F542 - Get HDD lightpath status（コンポーネントステータス信号の読み取り）
  - F543 Get SEL entry long text
  - F545 Get SEL entry text
  - F5B0 Set Identify LED
  - F5B1 Get Identify LED
  - F5B3 Get Error LED
  - F5DF Set Nonvolatile Cfg Memory to Default Values
  - F5E0 Set Configuration Space to Default Values
  - F5F8 Delete User ID

12.1.2 IPMI OEM コマンドの記述

この節では、個別の OEM 特有の IPMI コマンドについて説明します。

12.1.2.1 記述形式

本章で記載する OEM 特有の IPMI コマンドは、IPMI コマンドを記述するための IPMI 標準で使用する形式によって記述されます。

IPMI 標準では、各コマンドに対する入力パラメータと出力パラメータを一覧にしたコマンド表を使用して IPMI コマンドを記述します。

IPMI 標準の情報については以下のサイトを参照してください。

http://developer.intel.com/design/servers/ipmi/index.htm

12.1.2.2 SCCI 準拠の自動電源投入／電源切断コマンド

0115 Get Power On Source

本コマンドは最後に行われた自動電源投入の理由を返します。理由には以下にあげるものがあります。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**01** Cmd : コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**15** コマンド指定子
応答データ	-	**BC**
	-	**01**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	3	**01** データ長
	4	電源切断原因 : 最後の自動電源切断の理由

電源投入原因原因	**説明**
0x00	ソフトウェアまたはコマンド
0x01	電源スイッチ（フロントパネルまたはキーボード上）
0x02	電源障害後の自動再起動
0x03	クロックまたはタイマー（ハードウェア RTC またはソフトウェアタイマー）
0x04	ファン障害によるシャットダウン後の自動再起動
0x05	臨界温度によるシャットダウン後の自動再起動
0x08	ウォッチドックタイムアウト後の再起動
0x09	リモートオン（モデム RI ライン、SCSI ターミネーションパワー、LAN、IC カード リーダー・・・）
0x0C	CPU エラー後の再起動
0x15	ハードウェアリセットによる再起動
0x16	ウォームスタート後の再起動
0x1A	PCI バス電源管理イベントによる電源投入

電源投入原因原因	説明
0x1D	リモートマネージャ経由のリモート制御による電源投入
0x1E	リモートマネージャ経由のリモート制御による再起動／リセット

01 16 - Get Power Off Source

本コマンドは最後に行われた自動電源切断の理由を返します。理由には以下にあげるものがあります。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**01** Cmd : コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**16** コマンド指定子
応答データ	-	**BC**
	-	**01**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	3	**01** データ長
	4	電源切断原因 : 最後の自動電源切断の理由

電源切断原因	**説明**
0x00	ソフトウェア（SWOFF、コマンドによる電源切断）
0x01	電源スイッチ（フロントパネルまたはキーボード上）
0x02	AC 電源障害
0x03	クロックまたはタイマー（ハードウェア RTC またはソフトウェアタイマー）
0x04	ファン障害
0x05	臨界温度
0x08	ウォッチドッグタイムアウト繰り返し後の電源切断
0x0C	CPU エラー繰り返し後の電源切断
0x1D	リモートマネージャ経由のリモート制御による電源切断

_01 1C - Set Power Off Inhibit

本コマンドは*電源切断防止*フラグを設定し、サーバの電源が意図せずオフにされることを一時的に抑止します。

*電源切断防止*フラグを設定した場合、正当な理由なくサーバの電源をオフにしようとした場合に一時的に電源切断が防止されます。電源切断防止フラグが設定されていると、サーバの「Power Off」、「Power Cycle」または再起動を実行しようとした理由がファームウェアによって保存されますが、動作は実行されません。最後に実行したサーバの「Power Off」、「Power Cycle」または再起動の理由が常時保存されます。保存された動作は*電源切断防止*フラグをリセットしたときのみ実行されます。

*電源切断防止*フラグは、電源障害後、またはリセットボタンの押下時に自動的にリセットされます。

*電源切断防止*フラグには、メインメモリダンプを作成する際に使用するダンプフラグと同じ効果があります。この場合、ダンプを作成する前にイニシエーターで必ずフラグを設定し、ダンプが完了したときにリセットします。

要求データ	-	**B8** NetFnlLUN: OEM/ グループ
	-	**01** Cmd : コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**1C** コマンド指定子
	5	**00** オブジェクト ID
	6:7	**00 00** 値 ID
	8	**01** データ長
	9	電源切断防止フラグ : 0 = 防止しない、1 = 防止する
応答データ	-	**BC**
	-	**01**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

01 1D - Get Power Off Inhibit

本コマンドは*電源切断防止*フラグの値を取得します。

*電源切断防止*フラグの詳細については、381 ページ の「_01 1C - Set Power Off Inhibit」の説明を参照してください。

要求データ	-	**B8** NetFn|LUN: OEM/ グループ
	-	**01** Cmd : コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**1D** コマンド指定子
応答データ	-	**BC**
	-	**01**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	**01** 応答データ長
	6	電源切断防止フラグ : 0 = 防止しない、1 = 防止する

01 20 - Set Next Power On Time

本コマンドは、設定スペースに保存されている電源投入／切断時刻とは別に所定の時間でシステムの電源を投入します。

コマンドは 1 回のみ有効です。

前回 01 20 コマンドで設定した「電源投入」時刻をキャンセルするには、次の 01 20 コマンドで「0」を「電源投入」時刻に指定します。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**01** Cmd : コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**20** コマンド指定子
	5	**00** オブジェクト ID
	6:7	**00 00** 値 ID
	8	**04** データ長
	9:12	時刻（LSB ファースト）（下記参照）
応答データ	-	**BC**
	-	**01**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

時刻（LSB ファースト）

システムの電源を再度投入した時刻（UNIX 特有の形式）です。時刻は不揮発メモリに保存されません。設定単位は 1 分毎です。設定単位は 1 分毎です。システムの電源を投入した後、内部で時刻が 0 に 設定されます。
「電源投入」時刻に 「0 」を指定した場合、システムの電源は投入されません。

12.1.2.3 SCCI 準拠の通信コマンド

i SCCI 準拠の通信コマンドには、エージェントサービスが OS で起動していることが必要です。コマンドを実行するは、iRMC S4 と通信するエージェントが最終的に動作を行います。

02 05 - System OS Shutdown Request

本コマンドはサーバのオペレーティングシステムのシャットダウンを開始します。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**05** コマンド指定子
応答データ	-	**BC**
	-	**02**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

02 06 - System OS Shutdown Request and Reset

本コマンドはサーバのオペレーティングシステムのシャットダウンを開始した後にシステムを再起動します。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**06** コマンド指定子
応答データ	-	**BC**
	-	**02**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

02 08 - Agent Connect Status

本コマンドはエージェントがアクティブであるかどうかを確認します。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**08** コマンド指定子
応答データ	-	**BC**
	-	**02**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	**01** データ長
	6	**接続状態** : 00 =接続が切断された、エージェントが接続されていない 01 =接続が再確立された、エージェントが接続されている

02 09 Shutdown Request Cancelled

本コマンドは発行されたシャットダウン要求をキャンセルします。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**09** コマンド指定子
応答データ	-	**BC**
	-	**02**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

12.1.2.4 SCCI 準拠のシグナリングコマンド

10 02 - Write to System Display

本コマンドは、LocalView ディスプレイ（接続されている場合）に文字を書き込むために使用します。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**10** Cmd : コマンドグループファンテスト
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**02** コマンド指定子
	5	**オブジェクトインデックス** : : 書き込みを行うディスプレイの線
	6:7	**値 ID** （未使用）
	8	**長さ** 1 ずつ増加する書き込む文字数（文字列がヌル終端である必要はありません。ディスプレイの長さを超える文字列は切り捨てます。）
	9	**属性** 0 ＝文字列を左詰めで書き込みます 1 ＝文字列を右詰めで書き込みます
	10:10+n	ディスプレイに書き込む**文字**（文字列がヌル終端である必要はありません。）
応答データ	-	**BC**
	-	**10**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

12.1.2.5 Firmware 特有のコマンド

20 04 - Set Firmware Selector

本コマンドは、ファームウェアのリセット後にアクティブになる IRMC S4 のファームウェアイメージを設定します。

要求データ	-	**20** NetFnlLUN: ファームウェア
	-	**04** CMD ：コマンドグループファームウェア
	1	セレクタ： 0 ＝ Auto（版数が新しいファームウェアを選択します 。） 1 ＝ Low Firmware Image 2 ＝ High Firmware Image 3 ＝ Auto oldest version（版数が古いファームウェアを選択します 。） 4 ＝ MRP（書込日が新しいファームウェアを選択します。） 5 ＝ LRP（書込日が古いファームウェアを選択します。）
応答データ	-	**24**
	-	**04**
	1	完了コード

20 05 - Get Firmware Selector

本コマンドは現在のファームウェアセレクタ設定を返します。

要求データ	-	**20** NetFnlLUN: ファームウェア
	-	**05** CMD :コマンドグループファームウェア
応答データ	-	**24**
	-	**05**
	1	完了コード
	2	次回のブートセレクタ : 0 = Auto(最新のファームウェアバージョンの EEPROM を選択します。) 1 = Low EEPROM 2 = High EEPROM 3 = Auto oldest version(最も古いファームウェアバージョンの EEPROM を選択します。) 4 = MRP(最後に更新したファームウェアを選択します。) 5 = LRP(最初に更新したファームウェアを選択します。)
	3	動作中のセレクタ : どのファームウェアが現在動作中であるかを示します。 1 = Low EEPROM 2 = High EEPROM

C0 19 - Get Remote Storage Connection or Status

本コマンドは、渡されたパラメータに応じて、以下に関する情報を返します。

– 使用できるリモートストレージ接続があるか
– リモートストレージ接続の状態および種類

要求データ 1 が「1」に設定された場合、コマンドはストレージメディアがリモートストレージとして接続されているかどうかの情報を返します。

要求データ	-	**C0** NetFnlLUN: OEM
	-	**19** CMD : コマンドグループファームウェア
	1	01
	2	00
	3	00
応答データ	-	**C4**
	-	**19**
	1	完了コード
	2	**01**
	3	**00: 接続されていない** **01: 接続されている**
	4	**00**
	5	**00**

要求データ 1 が「2」に設定された場合、コマンドは任意のリモートストレージ接続の状態および種類に関する情報を返します。

要求データ	-	**C0** NetFnlLUN: OEM
	-	**19** CMD : コマンドグループファームウェア
	1	02
	2	00
	3	00 ＝接続 0 01 ＝接続 2
応答データ	-	**C4**
	-	**19**
	1	完了コード
	2	**02**
	3	**00**
	4	**00**
	5	**00 ＝無効／未知** **01 ＝アイドル** **02 ＝接続試行中** **03 ＝接続済み** **04 ＝接続再試行に失敗または試行回数の終了** **05** = **＝接続切断** **06** = **＝切断中**
	6	00 ＝無効／未知 **01 ＝ストレージサーバ／ IPMI** **02 ＝アプレット** **03 ＝なし／未接続**

C0 1A - Set Video Display On/Off

本コマンドは、ローカルコンソールの有効／無効を切り替えることができます。

要求データ	-	**C0** NetFnlLUN: OEM
	-	**1A** Cmd : コマンドグループファンテスト
	1	00 ＝ビデオ表示を有効に設定します 01 ＝ビデオ表示を無効に設定します
応答データ	-	**C4**
	-	**1A**
	1	完了コード

12.1.2.6 BIOS 特有のコマンド

F1 09 - Get BIOS POST State

本コマンドは BIOS が POST 中であるかどうかの情報を提供します。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**F1** Cmd : コマンドグループ BIOS
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**09** コマンド指定子
応答データ	-	**BC**
	-	**F1**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	[7:1] – 予備 [0] – BIOS POST 状態 : 0 ＝ BIOS が POST 状態ではありません。 1 ＝ BIOS が POST 状態です。

F1 15 - Get CPU Info

本コマンドは CPU 内部情報を返します。iRMC S4 では、POST フェーズ中に BIOS から本情報を取得します。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**F1** Cmd : コマンドグループ BIOS
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**15** コマンド指定子
	5	CPU のソケット番号（0 ベース）
応答データ	-	**BC**
	-	**F1**
	1	**完了コード** 01 ＝未実装の CPU ソケット
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5:6	CPU ID、LSB ファースト
	7	プラットフォーム ID
	8	ブランド ID
	9:10	CPU の最大コアスピード [MHz]、LSB ファースト
	11:12	Intel QuickPath インターコネクト [MT/s]、LSB ファースト
	13	熱制御オフセット
	14	熱ダイオードオフセット
	15	CPU データ予備
	16:17	記録 ID CPU 情報 SDR、LSB ファースト
	18:19	記録 ID CPU ファン制御 SDR、LSB ファースト
	20:21	CPU ID ハイワード、LSB ファースト（なければ 0）

12.1.2.7 iRMC S4 特有のコマンド

F5 10 - Get System Status

本コマンドは、電源状態、エラーステータス等のシステムの各種内部情報を返します。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : コマンドグループメモリ
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**10** コマンド指定子
	5:8	**タイムスタンプ**
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	**システムステータス** （詳細は、以下に参照してください。）
	6	**シグナリング** （詳細は、以下に参照してください。）
	7	**通知** （詳細は、以下に参照してください。）
	8	**POST コード**

i タイムスタンプは、*通知*バイトの評価のみに適用されます。

システム LED

Bit 7 - System ON

Bit 6 -

Bit 5 -

Bit 4 - SEL entries available

Bit 3 -

Bit 2 - Watchdog active

Bit 1 - Agent connected

Bit 0 - Post State

シグナリング

Bit 7 - Localize LED

Bit 6 -

Bit 5 -

Bit 4 -

Bit 3 - CSS LED

Bit 2 - CSS LED

Bit 1 - サーバのグローバルエラー LED

Bit 0 - サーバのグローバルエラー LED

通知

Bit 7 - SEL Modified （New SEL Entry）

Bit 6 - SEL Modified （SEL Cleared）

Bit 5 - SDR Modified

Bit 4 - Nonvolatile IPMI Variable Modified

Bit 3 - ConfigSpace Modified

Bit 2 -

Bit 1 -

Bit 0 - New Output on LocalView display

F5 12 - Get EEPROM Version Info

本コマンドは、EEPROM に保存されている現在のバージョン（bootloader、ファームウェアおよび ADR）に関する情報を返します。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : コマンドグループメモリ
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**12** コマンド指定子
	5	EEPROM# 00 = EEPROM 1、01 = EEPROM 2
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	**ステータス** 00 =チェックサムエラーランタイム FW、01 = OK
	6	**メジャー FW リビジョン** バイナリコード
	7	**マイナー FW リビジョン** BCD コード
	8:10	**Aux.FW Revision** バイナリコード（メジャー／マイナー／ Aux）
	11	**メジャー FW リビジョン** ASCII コード
	12	**メジャー SDRR リビジョン** BCD コード
	13	**マイナー SDRR リビジョン** BCD コード
	14	**SDRR リビジョン文字** ASCII コード
	15	**SDRR-ID** LSB バイナリコード
	16	**SDRR-ID** MSB バイナリコード
	17	**メジャー Booter リビジョン** バイナリコード
	18	**メジャー Booter リビジョン** BCD コード
	19:20	*Aux.Booter Revision* バイナリコード（メジャー／マイナー）

F5 42 - Get HDD lightpath status（コンポーネントステータス信号の読み取り）

このコマンドは、Hard Disk Drive（HDD）スロットの状態に関する情報を返します。

要求データ	-	**B8** NetFn|LUN: OEM/ グループ
	-	**F5** Cmd : コマンドグループ iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**42** コマンド指定子
	5	ステータス信号が読み取られるコンポーネントの**エントリ ID**（IPMI 1.5 Spec. の*表 37-12*）。
	6	ステータス信号が読み取られるコンポーネントの**エントリインスタンス**（0 ベース）。
	7	ステータス信号が関連するコンポーネントのステータスを報告するセンサの**センサタイプ**（IPMISpec. の*表 36-3*）。
	[8]	オプション（オプション） Bit 7:2 - 予約 Bit 1 : 完了コード 0x02 が削除される Bit 0 - 1 : コンポーネントステータスセンサのリターン ID 文字列
応答データ	-	**BC**
	-	**F5**
	1	**完了コード** 01 = ステータス信号を取得できません 02 = コンポーネントがありません
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	**信号状態**： 00 = OK 01 = 確認 02 = 故障前警告 03 = 故障
	6	**CSS と 物理 LED を使用可能**： Bit 6:0 - 0 = 物理 LED を使用不可 Bit 6:0 > 00 = 物理 LED を使用可能、単一または複数の色、コード Bit 7 = 0: CSS コンポーネントなし Bit 7 = 1 : CSS コンポーネント

[7]	コンポーネントステータスセンサの ID 文字列の長さ （リクエストバイト 8 の Bit 0 が設定されている場合のみ存在）
(8 ～ m)	コンポーネントステータスセンサの ID 文字列（ASCII 文字）の長さ （リクエストバイト 8 の Bit 0 が設定されている場合のみ存在）

F5 43 - Get SEL entry long text

本コマンドは任意の SEL エントリをロングテキストに変換します。

要求データ	-	**B8** NetFnlLUN: OEM/ グループ
	-	**F5** Cmd : コマンドグループ iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**43** コマンド指定子
	5:6	**レコード ID** SEL レコード 、LSB ファースト 0x0000: 最初のレコードを取得します。 0xFFFF: 最後のレコードを取得します。
	7	応答 SEL テキストの**オフセット**
	8	**MaxResponseDataSize** 応答の*変換済み SEL データ*サイズ（16:n）
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5:6	次のレコード ID
	7:8	**実際の ID**
	9	**レコードタイプ**
	10:13	**タイムスタンプ**
	14	**重大度 :** Bit 7: 0 = CSS コンポーネントなし 1 ＝ CSS コンポーネントあり Bit 6-4 : 000 ＝ INFORMAL 001 ＝ MINOR 010 ＝ MAJOR 011 ＝ CRITICAL 1xx ＝ Unknown’ Bit 3-0 : 予備、0000 とします。
	15	テキスト全体の**データ長**
	16:n	**変換済み SEL データ** 要求された部分 (n=16+ MaxResponseDataSize - 1)
	n + 1	**文字列終了** 「\0」という文字をつける

F5 45 - Get SEL Entry Text

本コマンドは任意のシステムイベントログ SEL エントリを ASCII テキストに変換します。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : コマンドグループ iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**45** コマンド指定子
	5:6	SDR の**レコード ID**、LSB ファースト
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5:6	**次のレコード ID**
	7:8	**実際の ID**
	9	**レコードタイプ**
	10:13	**タイムスタンプ**
	14	**重大度** : Bit 7: 0 = CSS コンポーネントなし 1 = CSS コンポーネントあり Bit 6-4 : 000 = INFORMAL 001 = MINOR 010 = MAJOR 011 = CRITICAL 1xx = Unknown’ Bit 3-0 : 予備、0000 とします。
	15	**データ長**
	16:35	**変換済み SEL データ**

F5 B0 - Set Identify LED

本コマンドにより、サーバオン／オフの識別灯（青色）を切り替えることが可能です。さらに、識別灯に直接接続された GPIO の設定および読み込みが可能になります。

i サーバ上の識別切り替えを使用して識別灯を切り替えることも可能です。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**B0** コマンド指定子
	5	**識別灯** : 0 ＝識別灯オフ 1 ＝識別灯オン
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

F5 B1 - Get Identify LED

本コマンドは、サーバの識別灯（青色）の状態に関する情報を返します。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**B1** コマンド指定子
応答データ	-	**BC**
	-	F5
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	識別灯の状態（ビット 0 のみが該当します。）

F5 B3 - Get Error LED

本コマンドは、サーバの Error LED（赤色）および CSS LED（黄色）の状態に関する情報を返します。Error LED はコンポーネントの最も重大なエラー状態を示します。CSS LED は、ユーザ自身が障害を修復できるかどうかを示します。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd ：コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**B3** コマンド指定子
応答データ	-	BC
	-	F5
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	**Error LED の状態**： 0 ＝ CSS off ／ GEL off 1 ＝ CSS off ／ GEL on 2 ＝ CSS off ／ GEL blink 3 ＝ CSS on ／ GEL off 4 ＝ CSS on ／ GEL on 5 ＝ CSS on ／ GEL blink 6 ＝ CSS blink ／ GEL off 7 ＝ CSS blink ／ GEL on 8 ＝ CSS blink ／ GEL blink

F5 DF - Reset Nonvolatile Cfg Variables to Default

本コマンドは、すべての不揮発性 IPMI 設定をデフォルト値に強制的に設定します。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**DF** コマンド指定子
	5:8	43 4C 52 AA = 'CLR'0xaa : セキュリティコード
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

F5 E0 - Reset ConfigSpace variables to default

本コマンドは、すべての設定スペース変数をデフォルトに強制的に設定します。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**E0** コマンド指定子
	5:8	43 4C 52 AA = 'CLR'0xaa : セキュリティコード
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

F5 F8 - Delete User ID

システムでは最大 16 人のユーザがサポートされます。本コマンドは、iRMC S4 ユーザを個別に削除することができます。

注意！

すべての iRMC S4 ユーザを削除するとシステムを管理することができなくなります。

要求データ	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**F8** コマンド指定子
	5:8	ユーザ ID（1 ～ 16）
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

12.2 SCCI およびスクリプト設定を使用した iRMC S4 の設定

この節では以下について説明します。

– HSCCI（**S**erverView **C**ommon **C**ommand **I**nterface）対応インターフェースを使用して iRMC S4 を設定する方法。

– iRMC S4 のスクリプト設定

12.2.1 iRMC S4 設定データ

i 以下で説明するインターフェースは主にリモート設定を行うためおもので、SCCI 実装では**ありません**。SCCI コマンドと設定の定義、および SCCI ファイルフォーマットのみ使用します。

12.2.1.1 概要

iRMC S4 は、NVRAM（不揮発性 RAM）の次の個別のセクションにある内部設定データを保存します。

– FTS 固有の ConfigSpace データ。ファームウェアが固定の内部記述テーブルまたはマッピングテーブルを使用してアドレス指定します。

– 製造メーカー固有のオリジナルの OMD NVCFG データ。オフセット定義でアクセスします。

オリジナルの OMD NVCFG データの設定データには、ConfigSpace アクセス手法でアクセスできるように、ファームウェアが内でマッピングされているものがあります。たとえば、iRMC S4 の DNS サーバと DNS 設定に、IPMI OEM LAN 設定パラメータおよび ConfigSpace を使用してアクセスできます。どちらの手法も、オリジナルの NVCFG 領域内の下位レベルの同じ構造にアクセスします。

iRMC S4 固有でない ServerView ソフトウェアコンポーネント（ServerView エージェントまたは Server Configuration Manager）は、標準の IPMI 関連のコマンド、および標準の IPMI ユーザ設定や IPv4 ネットワーク設定などの設定項目などをマッピングすることもあります。これにより、IPMI BMC 層と上位のソフトウェアレベル間に抽象化レベルを実装します。

SCCI は、Fujitsu が定義したジェネリックなアプリケーションプログラミングインターフェース（API）で、Server Management Controller ハードウェアおよび Server Management ソフトウェア（ServerView エージェントなど）に対応します。容易に拡張して、新しいコマンドや新しい設定項目に対応させることができます。SCCI のアーキテクチャの概要については、ServerView エージェントのオンラインヘルプを参照してください。

iRMC S4 は、iRMC S4 での */config URL* を使用したリモート設定と制限付きスクリプティングをサポートしています。

Web ベースのアクセスによる iRMC S4 のリモート設定の利点

Web ベースのアクセスによるリモート iRMC S4 設定には、次の利点があります。

– HTTP POST オペレーションを使用して、ファイルを iRMC S4 にアップロードできます。特別なツールは必要ありません。認証された HTTP POST オペレーションをサポートする任意のジェネリックツールやスクリプティング環境を使用できます。サンプルスクリプトが ServerView Suite DVD に収録されています。

– iRMC S4 Web サーバのビルトイン認証と認証手法を使用できます。

– ローカル iRMC S4 ユーザアカウントを使用する、RFC 2617 ベースの HTTP 1.1 Basic および Digest 認証をサポートします。

– 標準の HTTPS ベースのアクセスによるオプションの強力なビルトイン暗号化機能を装備しています。

– グローバルユーザアカウント（LDAP ディレクトリサーバによって管理されます）および HTTP 1.1 Basic 認証で使用できます。

  i HTTP 1.1 Basic 認証を使用する場合、暗号化と機密保持上の理由から、HTTPS プロトコルを使用してユーザ名とパスワードの組み合わせを保護するようにしてください。

– XML ベースの設定ファイルフォーマットを使用できます。手作業でファイルを編集するか、リファレンスインストールまたは Server Configuration Manager からファイルをエクスポートするかを選択できます。

  SCCI ベースのインストール手法（Server Configuration Manager など）で設定ファイルを再利用できます。

– 新しい設定項目と新しくサポートされる SCCI コマンドを容易に拡張できます。

12.2.1.2 SCCI ファイルフォーマット

> **i** 使用する XML 設定ファイル（*.pre*）のフォーマットは、Windows プラットフォームの ServerView エージェントと共にインストールされる、セットアップ設定ヘルプファイルから取得されます。この説明と iRMC S4 固有の注意事項のコピーを以下に示します。

設定ファイルは、次の XML 構文がベースとなります。

– 各構成設定は、「<CMD>」で始まるシンプルな XML フラグメントで構成されます。

– 構成設定の完全なシーケンスは、「<CMDSEQ> および </CMDSEQ>」というタグのペアで囲まれます。

以下に、2 つの構成設定で構成される典型的なコマンドシーケンスの例を示します。

```
<CMDSEQ>
<CMD Context="SCCI" OC="ConfigSpace" OE="3800" OI="0"
Type="SET">
<DATA Type="xsd::hexBinary" Len="1">04</DATA>
<CMD Context="SCCI" OC="ConfigSpace" OE="3801" OI="0"
Type="SET">
<DATA Type="xsd::hexBinary" Len="1">00</DATA> </CMD>
</CMDSEQ>
```

Context を内部で使用して、オペレーションプロバイダを選択します。現在、サポートされるプロバイダは SCCI のみです。

SCCI プロバイダ固有のコマンドのパラメータ

以下の SCCI プロバイダ固有のコマンドを使用できます。

Operation Code（OC）
コマンド／オペレーションコードを指定する 16 進値または文字列。

> i iRMC S4 は、制限された SCCI コマンドセットのみサポートします。サポートされるコマンドの一覧は、413 ページ の表「iRMC S4 でサポートされる SCCI コマンド」を参照してください。

Operation Code Extension（OE）
拡張されたオペレーションコードの 16 進値。デフォルト : OE=0

ConfigSpace 読み書きオペレーションには、この値で ConfigSpace ID を定義します。

Object Index（OI）
オブジェクトのインスタンスを選択する 16 進値。Default:OI=0"

Operation Code Type（Type）
構成設定の場合、値 GET（読み取りオペレーション）および SET（書き込みオペレーション）がサポートされます。デフォルト : Type=GET

> i SET にはデータが必要です。適切なデータタイプを指定するには、下記の *Data（DATA）*パラメータを使用します。

Cabinet Identifier（CA）
拡張キャビネットを選択して、そのキャビネット ID 番号を使用できます。

> i このパラメータをシステムキャビネットのリクエストに対して使用しないでください。

Data (`DATA`)

`SET` パラメータ（書き込みオペレーション）を指定する場合、データタイプ（`Type` パラメータ）と、場合によってはデータ長（`LEN` パラメータ）が必要です。

現在、以下のデータタイプがサポートされます。

– `xsd::integer`

  整数値

  例

  ```
  <DATA Type="xsd::integer">1234</DATA>
  ```

– `xsd::hexBinary`

  バイトストリーム。各バイトは 2 つの ASCII 文字でコード化されます。下記の例で示すように `Len` パラメータを使用して、ストリームの長さ（バイト数）を指定します。

  i データタイプ `xsd::hexBinary` は、制約なく使用できます。使用するバイト数は、*Len* パラメータで指定されます。

  例

  4 バイト `0x00 0x01 0x02 0x04` のストリームは、以下の ASCII ストリームとしてコード化されます。

  ```
  <DATA Type="xsd::hexBinary" Len="4">0001020304</DATA>
  ```

– `xsd::string`

  通常、文字列の転送に使用されます。また、`string` タイプは、IPv4 アドレスおよび MD5 ベースのユーザパスワードに使用できます。この場合、文字列データは、受け付けられるターゲットフォーマットに内部で変換されます。

  暗号化データの転送

  Fujitsu 専用のデータ暗号化は、ユーザまたはサービス（LDAP/SMTP）アクセスパスワードや、iRMC S4 の AVR ライセンスキーなどの機密データでサポートされます。*iRMC_PWD.exe* プログラムを使用して、パスワードデータを暗号化することができます（417 ページ の「iRMC_PWD.exe プログラムでの暗号化パスワードの生成」の項を参照）。

`Encrypted="1"` を `<DATA>` タグで設定して、書き込むデータを暗号化することを示す必要があります。

例

「Hello World」という文字列を転送する場合：

```
<DATA Type="xsd::string">Hello World</DATA>
```

クリア（読み取り可能）テキストとしてパスワードを転送する場合：

```
<DATA Type="xsd::string">My Readable Password</DATA>
```

暗号化されたパスワードを転送する場合：

```
<DATA Type="xsd::string"
Encrypted="1">TpVlTJwCyHEIsC8tk24ci83JuR9l</DATA>
```

IPv4 アドレス「192.23.2.4」を転送する場合 :

`<DATA Type="xsd::string">192.23.2.4</DATA>`

注意 !

`xsd::string` データタイプの使用は、読み込み可能な文字列、IP アドレス、MD5 ベースのユーザパスワードに限定されます。

その他のすべてのデータには、`xsd::hexbinary` データタイプを使用してください。

ä、ö、ü などの文字は、使用しているアプリケーションで実際に必要でない限り、文字列に直接指定しないでください。

SCCI および ConfigSpace インターフェースは、どちらも文字の暗号化情報を保存しません。つまり、US-ASCII 以外の文字は使用しているアプリケーションによって内部で解釈されるので、使用しないようにしてください。

特殊文字を実際に指定する必要がある場合、適切な BOM を含む UTF-8 フォーマットでファイルの編集と保存を行ってください。

Command Status（`Status`）

構成設定を転送すると、`Status` にオペレーションの結果が含まれます。オペレーションが正常終了した場合、値 `0` が返されます。

パブリックなすべての構成設定の仕様（ConfigSpace）については、*SCCI_CS.pdf* ファイルを参照してください。このファイルは、ServerView エージェントのインストールパッケージの *Help* フォルダの中にあります。また、*SCCI_CS.pdf* PRIMERGY Scripting Toolkit でも配布されます。

12.2.1.3 注意事項

.pre ファイルに指定されるすべてのコマンドは、通常順次に実行されます。以下については、このルールが除外されます。

– 壊れたネットワーク接続を回避するには、IPv4 および VLAN ネットワーク設定のコマンドをコマンドシーケンスの最後に実行します。

– 現在、IPv6 構成パラメータは、不揮発性の IPv6 構成パラメータの設定に限定されます。

  回避策として、次の手順を行うことができます。

  1. スクリプトを次のように調整します。

     a) スクリプトの開始時： IPv6 を無効します。

     b) IPv6 パラメータを設定します。

     c) スクリプトの終了時：Enable IPv6

  2. IPv4 アドレスからスクリプトを実行します。

– SSL 証明書と関連の一致するプライベートキーは、コマンドシーケンスの最後に実行されます。両方のコンポーネントは、同じ *.pre* ファイルに保存されている必要があり、互いに一致することが確認されます。

– 管理対象サーバのパワーマネジメントオペレーション、または iRMC S4 の再起動が必要な場合。

  個々のコマンドファイルでこれらのコマンドを実行するようにします（ただし、必須ではありません）。これを実現するには、設定オペレーションとパワーマネジメントオペレーションを別個のタスクに分割します。

– 連続するコマンドの実行間のオプションの時間遅延は、スクリプトの外部で実装します。

  たとえば、次の手順で実現することができます。

  1. スクリプトを別個のスクリプトに適切に分割します。

  2. クライアントの機能範囲を使用して、個々のファイルの送信間の時間遅延を挿入します。

12.2.1.4 iRMC S4 からのエクスポート /iRMC S4 へのインポート

iRMC S4 Web インターフェースの「*iRMC S4 ファームウェア設定の保存*」ページで、現在の iRMC S4 の設定データを設定ファイル（*.pre*）に保存（エクスポート）できます。また、既存の設定ファイル（*.pre*）の iRMC S4 設定データをインポートできます。つまり、iRMC S4 に設定データをロードできます（詳細は、166 ページ の「「iRMC S4 ファームウェア設定の保存」- ファームウェア設定の保存」の項を参照）。

あるいは、iRMC S4 設定をインポートするために、HTTP POST オペレーションを使用して、該当する SCCI コマンドファイルを iRMC S4 の */config URI* に送信することもできます。

12.2.2 iRMC S4 のスクリプト設定

この節では、以下のトピックについて説明します。

– iRMC S4 でサポートされる SCCI コマンド。
– iRMC S4 のスクリプト設定用のさまざまなスクリプト言語の使い方。
– *iRMC_PWD.exe* プログラムを使用した、暗号化パスワードの生成手順。

12.2.2.1 iRMC S4 でサポートされる SCCI コマンドの一覧

iRMC S4 でサポートされる SCCI コマンドを 表 22 に示します。

SCCI OpCode	SCCI コマンド文字列	説明
0xE002	ConfigSpace	ConfigSpace 書き込み
0x0111	PowerOnCabinet	サーバの電源オン
0x0112	PowerOffCabinet	サーバの電源オフ
0x0113	PowerOffOnCabinet	サーバのパワーサイクル
0x0204	ResetServer	サーバのハードリセット
0x020C	RaiseNMI	NMI パルス（マスク不可割り込み）
0x0205	RequestShutdownAndOff	グレースフルシャットダウン、実行中のエージェントが必要
0x0206	RequestShutdownAndReset	グレースフルリブート、実行中のエージェントが必要
0x0209	ShutdownRequestCancelled	シャットダウンリクエストのキャンセル
0x0203	ResetFirmware	BMC リセットの実行
0x0250	ConnectRemoteFdImage	Remote Image Mount（NFS または CIFS 共有）でフロッピーディスクイメージを接続 / 接続解除
0x0251	ConnectRemoteCdImage	Remote Image Mount（NFS または CIFS 共有）で CD/DVD .iso イメージを接続 / 接続解除
0x0252	ConnectRemoteHdImage	Remote Image Mount（NFS または CIFS 共有）でハードディスクイメージを接続 / 接続解除

表 22: iRMC S4 でサポートされる SCCI コマンド

12.2.2.2 cURL でのスクリプティング

オープンソースコマンドラインツール cURL で、URL 構文で指定したデータを転送できます。ソースコードの最新バージョンと、オペレーティングシステムのプリコンパイルバージョンは、http://curl.haxx.se/ からダウンロードできます。

以下に、curl を使用して設定ファイルを iRMC S4 に送信する方法についていくつかの例を示します。

> **i** curl コマンドラインオプションの詳細は、curl のマニュアルを参照してください。

– Basic 認証（デフォルト）とデフォルトの iRMC S4 admin アカウントでの HTTP Access

```
curl --basic -u admin:admin --data @Config.pre
http://<iRMC S4 IP address>/config
```

– Digest 認証とデフォルトの iRMC admin アカウントでの HTTP Access

```
curl --digest -u admin:admin --data @Config.pre
http://<iRMC S4 IP address>/config
```

– 認証チェックなし（-k）で、Digest 認証とデフォルトの iRMC admin アカウントでの HTTPS Access

```
curl --digest -k -u admin:admin --data @Config.pre
https://<iRMC S4 IP address>/config
```

– LDAP ユーザアカウントでの HTTPS Access

  LDAP ユーザには Basic 認証を指定する必要があることにご注意ください。

```
curl --basic -k -u LDAPuser:LDAPpassword --data @Config.pre
https://<iRMC S4 IP address>/config
```

12.2.2.3 Visual Basic（VB）スクリプトでのスクリプティング

次の VB スクリプトでは、設定ファイルを iRMC S4 に送信します。

```
IP_ADDRESS = "<iRMC S4 IP address>"
USER_NAME  = "admin"
PASSWORD   = "admin"

FILE_NAME  = ".\\ConfigFile.pre"

Const ForReading = 1
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objFile = objFSO.OpenTextFile(FILE_NAME, ForReading)
' -------------------------------------------------------------
On Error Resume Next

Set xmlHttp = CreateObject("Microsoft.XMLHTTP")
xmlHttp.Open "POST", "http://" & IP_ADDRESS & "/config", False,
USER_NAME, PASSWORD
xmlhttp.setRequestHeader "Content-Type", "application/x-www-
form-urlencoded"
xmlHttp.Send objFile.ReadAll

Wscript.Echo xmlhttp.responsexml.xml
```

12.2.2.4 Python でのスクリプティング

```
#!/usr/bin/python3
import sys
import httplib2
from urllib.parse import urlencode

# ===============================================================
# iRMC

USER = 'admin'
PWD  = 'admin'
IP_ADDR =  '192.168.1.100'
# ===============================================================

h = httplib2.Http()

# Basic/Digest authentication
h.add_credentials(USER, PWD)

def doit(data,ausgabe=sys.stdout):
  try:
    resp, content = h.request("http://%s/config" % IP_ADDR,
    "POST", data)
    if resp['status'] == '200'
      data = content.decode('utf-8')
      print(data,file=ausgabe)
      else:
      print('STATUS:',resp['status'],file=ausgabe)
      print(str(resp),file=ausgabe)
  except Exception as err:
    print('ERROR:',str(err),file=ausgabe)
  print()


# Example 1 - send a configuration file to the iRMC S4
try:
  data = open('ConfigFile.pre').read()
  doit(data)
except Exception as err:
  print('ERROR:',str(err),file=ausgabe)


# Example 2 - Set Config Space Values
# 0x200 (ConfCabinetLocation) and
# 0x204 (ConfSystemContact) direct from the script
#
LocationContact = '''<?xml version="1.0" encoding="UTF-8"
standalone="yes" ?>
```

```
<CMDSEQ>
  <!-- ConfCabinetLocation -->
  <CMD Context="SCCI" OC="ConfigSpace" OE="200" OI="0" >
    <DATA Type="xsd::string">%s</DATA>
  </CMD>
  <!-- ConfSystemContact -->
  <CMD Context="SCCI" OC="ConfigSpace" OE="204" OI="0" >
    <DATA Type="xsd::string">%s</DATA>
  </CMD>
</CMDSEQ>
'''

doit(LocationContact % ("Ostsee","Kiel"))
```

12.2.2.5 iRMC_PWD.exe プログラムでの暗号化パスワードの生成

Fujitsu Technology Solutions iRMC パスワード暗号化および確認ユーティリティ *iRMC_PWD.exe* は、SCCI スクリプティングで使用するための暗号化パスワードを生成できる Win32 プログラムです。*iRMC_PWD.exe* を使用して、シングルパスワードの暗号化と、スクリプト設定用の SCCI バッチファイルの生成の両方を行うことができます。

iRMC_PWD 標準コマンドオプション

[-h] [-?]

このヘルプ。

[-v]

暗号化されたパスワード文字列を確認します。

[-o] <oid>

暗号化するデータのオブジェクト ID。

[-u] <username>

指定したオブジェクト ID のユーザ名（オプション）。

[-p] <password>

指定したオブジェクト ID のパスワード // 確認する暗号化パスワード文字列。

[-x] <opCodeExt>

暗号化する ConfigSpace データの Opcode 拡張。

[-p] <password>

指定したオブジェクト ID のパスワード。
デフォルト：1452 (ConfBMCAcctUserPassword)

サポートされる値：

1452 - ConfBMCAcctUserPassword

1273 - ConfAlarmEmailSMTPAuthPassword

197A - ConfLdapiRMCgroupsUserPasswd

502 - ConfBmcRadiusSharedSecret

1A52 - ConfBmcRemoteFdImageUserPassword

1A62 - ConfBmcRemoteCdImageUserPassword

1A72 - ConfBmcRemoteHdImageUserPassword

1980 - ConfBMCLicenseKey

iRMC_PWD コマンドライン出力オプション

[-b]

出力ファイルを WinSCU BATCH ファイルとして作成します。

[-f] <Output File>

出力ファイルの名前を指定します。
デフォルト : *iRMC_pwd.txt*
バッチモードのデフォルト：*iRMC_pwd.pre*

例

oid *2* を使用して、ユーザ名を `admin` に、パスワードを `SecretPassword` に設定／変更する `.pre` ファイルを生成するとします。

これを実現するには、以下のコマンドを入力します。

```
iRMC_PWD -o 2 -u admin -p SecretPassword -b
```

iRMC_PWD が、419 ページ の図 212 に示される内容を使用して、*.pre* ファイルを生成します。

```
iRMC_PWD -o 2 -u admin -p SecretPassword -b


<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<CMDSEQ>
<!-- "ConfBMCAcctUserName" -->
<CMD Context="SCCI" OC="ConfigSpace" OE="1451" OI="2" Type="SET">
  <DATA Type="xsd::string">admin</DATA>
  <STATUS>0</STATUS>
</CMD>
<!-- "ConfBMCAcctUserPassword" -->
<CMD Context="SCCI" OC="ConfigSpace" OE="1452" OI="2" Type="SET">
  <DATA Type="xsd::string"
Encrypted="1">N2BZd3oLHAgc11pnHCAV9P/ItwRue4qBB3IU7Xsh</DATA>
  <STATUS>0</STATUS>
</CMD>
</CMDSEQ>
```

図 212: 生成される .pre ファイルの内容